

**UKUROVA NİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

YÜKSEK LİSANS TEZİ

Nİl MANSUROĞLU

GRÖBNER BAZI VE İNDİRGEME TEKNİKLERİ

MATEMATİK ANABİLİM DALI

ADANA,2009

ÖZ

YÜKSEK LİSANS TEZİ

GRÖBNER BAZI VE İNDİRGEME TEKNİKLERİ

NİL MANSUROĞLU

ÇUKUROVA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

Danışman: Yrd.Doç.Dr.Zerrin ESMERLİGİL

Yıl:2009, Sayfa:67

Jüri: Yrd.Doç.Dr.Zerrin ESMERLİGİL

Prof.Dr.Naime EKİCİ

Yrd.Doç.Dr.Perihan ARTUT (DİNÇ)

$K[x_1, x_2, \dots, x_n]$, K cismi üzerinde n değişkenli polinom cebiri ve $G = \{g_1, g_2, \dots, g_t\}$, $K[x_1, x_2, \dots, x_n]$ de sıfırdan farklı elemanlara sahip bir küme olsun. Bu tezde G kümesinin gröbner bazı olup olmadığını belirleyen gerek ve yeter koşullar incelenmiştir. Pik indirgeme tekniği ile $ax^n + by^m + \sum_{im+jn \leq mn} c_{ij}x^i y^j$ formundaki polinomlar sınıflandırılarak iki değişkenli polinomların bir sınıflandırması sağlandı.

Anahtar Kelimeler: Polinom cebiri, gröbner bazı, S-polinomu, pik indirgeme tekniği.

ABSTRACT
MSc THESIS

GROBNER BASES AND REDUCTION TECHNIQUES

Nil MANSUROĞLU

DEPARTMENT OF MATHEMATICS
INSTITUTE OF NATUREL AND APPLIED SCIENCES
UNIVERSITY OF ÇUKUROVA

Supervisor: Assist. Prof. Dr. Zerrin ESMERLİĞİL
Year: 2009, Pages: 67
Jury: Assist. Prof. Dr. Zerrin ESMERLİĞİL
Prof. Dr. Naime EKİCİ
Assist. Prof. Dr. Perihan ARTUT (DİNÇ)

Let $K[x_1, x_2, \dots, x_n]$ be the polynomial algebra in n variables over a field K and $G = \{g_1, g_2, \dots, g_t\}$ be a set of non-zero polynomials in $K[x_1, x_2, \dots, x_n]$. In this thesis we have analyzed necessary and sufficient conditions determining whether the given a set G is grobner basi. K . On the other hand using peak reduction technique, we have contributed toward a classification of two variables polynomials having classified, up to an automorphism, polynomials of the form $ax^n + by^m + \sum_{im+jn \leq mn} c_{ij}x^i y^j$.

Key Words: Polynomial algebra, grobner bases, S -polynomial, peak reduction technique.

TEŞEKKÜR

Bu çalışmamın hazırlanmasında bilgi ve tecrübeleri ile beni aydınlatan,her aşamasında yardımlarını esirgemeyen ve değerli zamanlarını ayırarak çalışmamın tamamlanmasını sağlayan saygıdeğer hocalarım sayın Prof.Dr.Naime EKİCİ ve sayın Yrd.Doç.Dr.Zerrin ESMEİLİĞİL'e sonsuz şükran ve teşekkürlerimi sunarım. Ayrıca değerli arkadaşlarım Hüda DOĞAN'a, Özer CAN'a, Arş.Gör.Demet (PARLAK) SÖNMEZ'e, Arş.Gör.Nazar Şahin ÖĞÜŞLÜ'e ve tüm Matematik Bölümü akademik personeline bu çalışmanın oluşmasında yardımlarını esirgemedikleri için teşekkürlerimi sunarım. Tez yazımında bana yardımcı olan kardeşlerim Necim MANSUROĞLU'na, Doğan MANSUROĞLU'na, Ebru MANSUROĞLU'na, bugüne kadar beni sürekli destekleyen ve her zaman yanımda olan annem Makbule MANSUROĞLU'na ve babam Ahmet MANSUROĞLU'na teşekkür ederim.

İÇİNDEKİLER

SAYFA

ÖZ.....	I
ABSTRACT.....	II
TEŞEKKÜR.....	III
İÇİNDEKİLER.....	IV
1.GİRİŞ.....	1
2.TEMEL TANIM VE TEOREMLER.....	3
2.1.Gröbner Bazı.....	3
2.2.Temel Otomorfizm ve Peak Reduction.....	18
3.GRÖBNER BAZININ TEMEL UYGULAMALARI.....	20
3.1 Gröbner Bazı.....	20
3.2.S-Polinomları.....	25
3.3.Gröbner Bazı ile İlgili Uygulamalar.....	32
4.PİK İNDİRGEME TEKİNİĞİ.....	47
4.1.Değişmeli Cebirde Pik İndirgeme Tekniği.....	47
4.2.Temel Otomorfizm ve Pik İndirgemesi.....	50
4.3.Polinom Otomorfizmlerinin Grubunun Parçalanışı.....	56
KAYNAKLAR.....	59
ÖZGEÇMİŞ.....	61

1. GİRİŞ

Pik indirgeme metodu teorik bilgisayar biliminde olduğu gibi matematiğin farklı birçok alanında kullanılan bir tekniktir. Bu teknik Whitehead [14] tarafından tanımlandı. Whitehead [14], bu tekniği bir serbest grubun otomorfizmlerini ilgilendiren algoritmik problemleri çözmek için kullandı. Ayrıca bu yöntem grup teorisi, topoloji ve diğer bazı alanlarda birçok problemin çözümünde kullanıldı.

Bu tezde, Pik indirgeme tekniğinin, değişmeli cebir ve afin cebir geometrisindeki ilk uygulamalarını inceleyeceğiz. Kullanılan bu teknik,

$$ax^n + by^m + \sum_{im+jn \leq mn} c_{ij} x^i y^j$$

formundaki polinomları sınıflandırarak iki değişkenli polinomların bir sınıflandırmasını sağlar.

Bu teknik genellikle verilen bir T dönüşümler grubunun işlemi altında verilen bir P nesnesinin kompleksinin kanonik formunu bulmada kullanılır.

2. Bölümde tez boyunca kullanılan tanımlar ve bazı teoremler verildi.

3.Bölümde Gröbner bazı incelendi. Gröbner bazı 1965 yılında Bruno Buchberger [2] tarafından tanımlandı. $K[x_1, x_2, \dots, x_n]$, K cismi üzerinde n değişkenli polinom cebiri ve sıfırdan farklı elemanlara sahip bir $G = \{g_1, g_2, \dots, g_t\}$ kümesi olsun. Eğer her $f \in I - \{0\}$ ve en az bir $i \in \{1, 2, \dots, t\}$ için $lm(g_i)/lm(f)$ ise G kümesine bir gröbner bazı denir. Birbirlerine denk koşullar verilerek $K[x_1, x_2, \dots, x_n]$ n değişkenli bir polinom cebirinin G gröbner bazı elde edildi. Eğer $G = \{g_1, g_2, \dots, g_t\} \subset K[x_1, x_2, \dots, x_n]$ olmak üzere G , bir gröbner bazı ise her $f \in K[x_1, x_2, \dots, x_n]$ için G ile bölümünden kalan teriminin tek olduğu gösterildi. Ayrıca bu bölümde gröbner bazının temel uygulamaları verildi.

4. Bölümde Pik indirgeme tekniğinin değişmeli cebir ve afin cebir geometrisindeki uygulamaları incelendi. Pik indirgeme tekniği matematiğin farklı birçok alanında ve bir serbest grubun otomorfizmleri ile ilgili algoritmik problemleri

çözmek için kullanıldı. $K[x, y]$, K cismi üzerinde iki değişkenli polinom cebiri olsun. Pik indirgeme tekniği kullanılarak $ax^n + by^m + \sum_{im+jn \leq mn} c_{ij}x^i y^j$ formundaki polinomları sınıflandırarak iki değişkenli polinomların bir sınıflandırması sağlandı.

2. TEMEL TANIM VE TEOREMLER

Bu kısımda gröbner bazı ve pik indirgeme tekniği ile ilgili temel tanım ve teoremleri vereceğiz.

$K[x_1, x_2, \dots, x_n]$, K cismi üzerinde n değişkenli polinom cebiri ve $T^n = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mid \alpha_i \in N, i = 1, 2, \dots, n\}$ bazıyla bir K -vektör uzayı olsun.

2.1.Gröbner Bazı

Tanım 2.1.1: K , bir cisim olsun. n değişkenli polinomlar kümesini $K[x_1, x_2, \dots, x_n]$ ile gösterelim. $K[x_1, x_2, \dots, x_n]$, değişmeli bir halkadır. Aynı zamanda $K[x_1, x_2, \dots, x_n]$ kümesi, $T^n = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mid \alpha_i \in N, i = 1, 2, \dots, n\}$ bazıyla bir K -vektör uzayıdır.

$K^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in K\}$ kümesine afin n -uzayı denir.

$K = R$ alınırsa R^n öklit uzayı elde edilir. Verilen bir $f \in K[x_1, x_2, \dots, x_n]$ polinomu, K^n den K 'ya aşağıdaki şekilde bir fonksiyon tanımlar.

$$\begin{aligned} K^n &\xrightarrow{f} K \\ (a_1, a_2, \dots, a_n) &\longrightarrow f(a_1, a_2, \dots, a_n) \end{aligned}$$

Bu fonksiyon evaluasyon diye adlandırılır.

Örneğin; $f \in K[x, y]$, $f = x.y$

$$\begin{aligned} K^2 &\xrightarrow{f} K \\ (5, 2) &\longrightarrow f(5, 2) = 5.2 = 10 \in K \end{aligned}$$

Tanım 2.1.2: $f \in K[x_1, x_2, \dots, x_n]$ olsun.

$V(f) = \{(a_1, a_2, \dots, a_n) \mid f(a_1, a_2, \dots, a_n) = 0\}$ kümesine f 'nin sınıfı denir.

Örnek 2.1.1: $f = x^2 + y^2 - 1 \in R[x, y]$ için $V(f)$ kümesini yazalım.

$V(f) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 - 1 = 0\}$ kümesi xy düzleminde merkezi $(0,0)$, yarıçapı 1 olan bir çemberdir.

Tanım 2.1.3: $f_1, f_2, \dots, f_s \in K[x_1, x_2, \dots, x_n]$ için

$$V(f_1, f_2, \dots, f_s) = \{(a_1, a_2, \dots, a_n) \mid f_i(a_1, a_2, \dots, a_n) = 0, 1 \leq i \leq s\}$$

olarak tanımlanır. Dikkat edilecek olursa

$$V(f_1, f_2, \dots, f_s) = \bigcap_{1 \leq i \leq s} V(f_i)$$

dir.

Daha genel olarak $S \subseteq K[x_1, x_2, \dots, x_n]$ ise

$$V(S) = \{(a_1, a_2, \dots, a_n) \mid f(a_1, a_2, \dots, a_n) = 0, \forall f \in S\}$$

dır.

Örnek 2.1.2: $V(x^2 + y^2 - 1, x - 3y^2)$ kümesini belirleyelim.

$$x^2 + y^2 - 1 = 0 \text{ (0,0) merkezli, 1 yarıçaplı çember}$$

ve

$$x - 3y^2 = 0 \text{ } xy \text{ düzleminde bir parabol olup}$$

$V(x^2 + y^2 - 1, x - 3y^2)$ bu her iki eğri üzerinde bulunan tüm noktaların kümesidir.

$f_1, f_2, \dots, f_s \in K[x_1, x_2, \dots, x_n]$ olmak üzere $f_1, f_2, \dots, f_s$ polinomları tarafından üretilen ideali $I = \langle f_1, f_2, \dots, f_s \rangle$ ile göstereceğiz.

Lemma 2.1.1: $I = \langle f_1, f_2, \dots, f_s \rangle$, $K[x_1, x_2, \dots, x_n]$ de bir ideal olsun.

$$V(I) = V(f_1, f_2, \dots, f_s)$$

dir.

İspat: $a \in V(I)$ olsun. Her $f \in I$ için $f(a) = 0$, $f_i \in I$ için $f_i(a) = 0$ ise $a \in V(f_1, f_2, \dots, f_s)$ dir. $V(I) \subseteq V(f_1, f_2, \dots, f_s)$ olur.

$a \in V(f_1, f_2, \dots, f_s)$ olsun. $f \in I$ olsun.

$f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s$ olsun. $u_i \in K[x_1, x_2, \dots, x_s]$, $1 \leq i \leq s$

$f(a) = (u_1 f_1 + u_2 f_2 + \dots + u_s f_s)(a)$

$f(a) = u_1(a)f_1(a) + u_2(a)f_2(a) + \dots + u_s(a)f_s(a) = 0$

$a \in V(I)$ olur.

$V(f_1, f_2, \dots, f_s) \subseteq V(I)$

Sonuç olarak $V(I) = V(f_1, f_2, \dots, f_s)$ dır.

Örnek 2.1.3: $L = \langle x + y, x \rangle$, $I = \langle x, y \rangle$, $J = \langle x + xy, x^2, y^2, y + xy \rangle$ kümeleri $K[x, y]$

de birer ideal olsun. $L = I = J$ olduğunu gösterelim.

$x, y \in J$ olup olmadığını göstermeliyiz.

$(x + xy) - (y + xy) = x - y \in J$ ise $(x - y)^2 \in J$

$$\underbrace{x^2}_{\in J} + \underbrace{y^2}_{\in J} - \underbrace{2xy}_{\in J} \in J$$

$$-2xy \in J \quad \text{ise} \quad -xy \in J$$

$$x + xy - xy = x \in J, \quad y + xy - xy = y \in J$$

Önerme 2.1.1. $\langle f_1, f_2, \dots, f_s \rangle = \langle f'_1, f'_2, \dots, f'_s \rangle$ ise

$$V(f_1, f_2, \dots, f_s) = V(f'_1, f'_2, \dots, f'_s)$$

dir.

İspat: Bu önermenin ispatı [2] de verilmiştir.

Teorem 2.1.1: (Hilbert Baz Teoremi) [2]

R , değişmeli bir halka olsun. Aşağıdakiler birbirlerine denktir.

i) I , R 'nin herhangi bir ideali ise öyle $f_1, f_2, \dots, f_s \in R$ vardır ki

$I = \langle f_1, f_2, \dots, f_s \rangle$ dir.

ii) Eğer $I_1 \subseteq I_2 \subseteq \dots \subseteq I_N \subseteq \dots$ R de artan bir idealler zinciri ise bir N için $I_N = I_{N+1} = I_{N+2} = \dots$ dir.

İspat: I , R nin bir ideali ve $I = \langle f_1, f_2, \dots, f_s \rangle$ olsun.

$J = \bigcup_{i=1}^{\infty} I_i$ idealini alalım.

(i) den dolayı $J = \langle f_1, f_2, \dots, f_s \rangle$ olacak şekilde $f_1, f_2, \dots, f_s \in R$ dir. O zaman bir N için $f_1, f_2, \dots, f_s \in I_N$ dir. Böylece $I_N = I_{N+1} = I_{N+2} = \dots$ olur.

Şimdi tersine $I_1 \subseteq I_2 \subseteq \dots \subseteq I_N \subseteq \dots$ R de artan idealler zinciri ve bir N için $I_N = I_{N+1} = I_{N+2} = \dots$ olsun.

I 'nın, R 'de sonsuz üreteçli bir ideali olduğunu varsayalım.

$f_1 \in I$ alalım. $\langle f_1 \rangle \neq I$ dir.

$f_2 \in I / \langle f_1 \rangle$ alalım. $\langle f_1 \rangle \subset \langle f_1, f_2 \rangle \neq I$ dir.

$f_3 \in I / \langle f_1, f_2 \rangle$ alalım. $\langle f_1 \rangle \subset \langle f_1, f_2 \rangle \subset \langle f_1, f_2, f_3 \rangle \neq I$ dir.

$\vdots$

Bu şekilde sonsuz artan zinciri elde edilir. Hipotezden bir s için $I = \langle f_1, f_2, \dots, f_s \rangle$ olup I 'nın sonlu üreteçli olduğu görülür.

Tanım 2.1.4: R , birim elemanlı ve değişmeli bir halka olsun. Eğer R , Teorem 2.1.1. deki koşullardan birini sağlıyorsa R 'ye bir Noetherian halkası denir.

Teorem 2.1.2: R , bir Noetherian halka ise $R[x]$ de bir Noetherian halkasıdır.

Sonuç 2.1.1: K bir cisim ise $K[x_1, x_2, \dots, x_n]$ bir Noetherian halkasıdır.

Tanım 2.1.5: $x^\alpha, x^\beta \in T^n$ olsun. Bir sıralamanın tam sıralama olması için $x^\alpha < x^\beta$, $x^\alpha = x^\beta$ veya $x^\alpha > x^\beta$ olması gerekir. Ayrıca $g, f \in K[x_1, x_2, \dots, x_n]$ ve $lm(g)$, $lm(f)$ 'den daha küçük olmak üzere $f \xrightarrow{g} r$ şeklinde f, g 'ye göre r 'ye indirgenir. r 'nin derecesi g 'nin derecesinden küçüktür. Böylece bu indirgeme sonludur ve bu sıralama iyi sıralama olur. Bütün bu koşulları sağlayan sıralamaya terim sıralaması denir.

Tanım 2.1.6: T^n , vektör uzayını düşünelim. Aşağıdaki koşullar sağlanırsa T^n üzerindeki bir "terim sıralama" sına, "<" tam sıralamadır denir. Terim sıralamasına göre $x < x$, $x < y$ yada $y < x$ dir. $x < y$ ve $y < z$ ise $x < z$ dir.

1) $1 < x^\alpha, \forall x^\alpha \in T^n, x^\alpha \neq 1$ ise

2) Eğer $x^\alpha < x^\beta$ ise $x^\alpha x^\gamma < x^\beta x^\gamma, \forall x^\gamma \in T^n$,

$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ ise $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in N^n, \alpha_i \in N, 1 \leq i \leq n$.

Tanım 2.1.7: T^n üzerinde $x_1 > x_2 > \dots > x_n$ ve $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \dots, \beta_n) \in N^n$ olsun. Eğer iki farklı α_i ve β_i koordinatlarından soldan ilk bileşenden başlayarak $\alpha_i < \beta_i$ koşulu sağlanırsa bu sıralamaya alfabetik sıralama denir. Bu sıralamaya kısaca lex sıralaması diyelim.

Örneğin, lex sıralamasına göre $x_1^2 < x_1^2 x_2^5$ olur.

Tanım 2.1.8: $x_1 > x_2 > \dots > x_n$ olsun.

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$

$\beta = (\beta_1, \beta_2, \dots, \beta_n)$ olmak üzere eğer

$x^\alpha < x^\beta \Leftrightarrow \sum \alpha_i < \sum \beta_i$ yada $\sum \alpha_i = \sum \beta_i$ ise $x^\alpha < x^\beta$ (lex'e göre) ise bu sıralamaya dereceye göre alfabetik sıralama denir. Bu sıralamayı dlex ile göstereceğiz.

Örneğin; dlex sıralamasına göre $x_1^2 x_2 < x_2^4$,

lex sıralamasına göre $x_1^2 x_2 > x_2^4$ dir.

Tanım 2.1.9: $x_1 > x_2 > \dots > x_n$ olsun.

$x^\alpha < x^\beta \Leftrightarrow \sum \alpha_i < \sum \beta_i$ yada $\sum \alpha_i = \sum \beta_i$ ve sağda karşılaştırma yapıldığında derecesi büyük olan daha küçüktür şeklindeki sıralamaya dereceye göre ters yönde alfabetik sıralama denir. Bu sıralamayı drlex ile göstereceğiz.

Örneğin; dlex sıralamasına göre $x_1^2 x_2 x_3 > x_1 x_2^3$,

drlex sıralamasına göre $x_1^2 x_2 x_3 < x_1 x_2^3$ dir.

Not: $K[x_1, x_2]$ 'de drlex ile dlex eşdeğerdir.

İspat: $x^\alpha = x_1^a x_2^b$, $x^\beta = x_1^c x_2^d$ $a + b = c + d$ olsun.

$$\begin{aligned} x^\alpha < x^\beta \text{ (dlex)} &\Leftrightarrow x_1^a x_2^b < x_1^c x_2^d \\ &\Leftrightarrow a < c \text{ olduğundan } a - c < 0 \\ &\Leftrightarrow a - c = d - b < 0, d < b \\ &\Leftrightarrow x_1^a x_2^b < x_1^c x_2^d \text{ (drlex)} \\ &\Leftrightarrow x^\alpha < x^\beta \text{ (drlex)} \end{aligned}$$

dir.

Önerme 2.1.2: $f, g \in K[x_1, x_2, \dots, x_n]$ için $f = h.g$ olacak şekilde bir $h \in K[x_1, \dots, x_n]$ varsa g/f yazacağız. $x^\alpha, x^\beta \in T^n$ ve $\leq$ bir terim sıralaması olsun. Bu durumda x^α, x^β yı böler ise $x^\alpha \leq x^\beta$ dir.

İspat: $x^\beta = x^\alpha x^\gamma$ olacak şekilde $x^\gamma \in T^n$ olsun. $1 \leq x^\gamma$ ise $x^\alpha \leq x^\alpha x^\gamma = x^\beta$ dir. Böylece $x^\alpha \leq x^\beta$ dir.

Önerme 2.1.3: T^n üzerindeki her terim sıralama bir iyi sıralamadır. Her $A \subset T^n$ ve her $x^\beta \in A$ için $x^\alpha \in A$ vardır ve $x^\alpha \leq x^\beta$ dir.

Tanım 2.1.10: $f \in K[x_1, x_2, \dots, x_n]$ ve $f = a_1 x^{\alpha_1} + a_2 x^{\alpha_2} + \dots + a_r x^{\alpha_r}$ olsun. Burada $x^{\alpha_i} \in T^n, a_i \in K, \alpha_i \in N^n$ dir. $x^{\alpha_1} > x^{\alpha_2} > \dots > x^{\alpha_r}$ varsayalım.

$$1) f \text{ nin en büyük dereceli monomiali } lm(f) = x^{\alpha_1}$$

$$\text{veya } f \text{ nin en büyük dereceli kuvvet çarpımı } lp(f) = x^{\alpha_1}$$

$$2) f \text{ 'nin en büyük dereceli katsayısı } lc(f) = a_1$$

$$3) f \text{ 'nin en büyük dereceli terimi } lt(f) = a_1 x^{\alpha_1}$$

şeklinde tanımlanır.

Not: $f, g \in K[x_1, x_2, \dots, x_n]$ için

$$lp(0) = lc(0) = lt(0) = 0,$$

$$lp(f.g) = lp(f).lp(g),$$

$$lc(f.g) = lc(f).lc(g),$$

$$lt(f.g) = lt(f).lt(g)$$

dir.

Örnek 2.1.4: $f = 2x^2yz + 3xy^3 - 2x^3$ ve $x > y > z$ olsun.

1) lex sıralamasına göre

$$lp(f) = x^3$$

$$lc(f) = -2$$

$$lt(f) = -2x^3$$

dır.

2) deglex sıralamasına göre

$$lp(f) = x^2yz$$

$$lc(f) = 2$$

$$lt(f) = 2x^2yz$$

dır.

3) degrlex sıralamasına göre

$$lp(f) = xy^3$$

$$Ic(f) = 3$$

$$It(f) = 3xy^3$$

dır.

Tanım 2.1.11: $f, g, h \in K[x_1, x_2, \dots, x_n]$ olsun. Eğer $lm(g)$, f deki bir m terimini bölerse ve

$$h = f - \frac{m}{lt(g)}g \text{ ise } f, \text{ modulo } g \text{ 'ye göre bir adımda } h \text{ 'ye indirgenmiştir}$$

denir ve $f \xrightarrow{g} h$ ile gösterilir.

Örnek 2.1.5: $Q[x, y]$ 'de $f = 6x^2y - x + 4y^3 - 1$, $g = 2xy + y^3$ polinomlarını alalım. $x > y$ olsun.

lex sıralamasına göre

$$lm(g) = xy/6x^2y$$

$$h = f - 3xg = 6x^2y - x + 4y^3 - 1 - 3x(2xy + y^3)$$

$$h = -x + 4y^3 - 1 - 3xy^3$$

$$lm(h) = xy^3$$

$$f \xrightarrow{g} h \text{ olur.}$$

dlex sıralamasına göre

$$lm(g) = y^3/4y^3$$

$$h = f - 4g = 6x^2y - x + 4y^3 - 1 - 8xy - 4y^3$$

$$h = 6x^2y - x - 1 - 8xy$$

olur.

Tanım 2.1.12: $f, h, f_1, f_2, \dots, f_s \in K[x_1, x_2, \dots, x_n]$ ve $F = \{f_1, f_2, \dots, f_s\}$ olsun. Eğer

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \longrightarrow \dots \longrightarrow h_{t-1} \xrightarrow{f_{i_t}} h$$

olacak şekilde bir $i_1, i_2, \dots, i_t \in \{1, 2, \dots, s\}$ indis kümesi ve $h_1, h_2, \dots, h_{t-1} \in K[x_1, x_2, \dots, x_n]$ polinomları varsa f , modulo F 'ye göre h 'ye indirgenir denir ve $f \xrightarrow{F} h$ ile gösterilir.

Örnek 2.1.6: $Q[x, y]$ 'de $f = y^2x$, $f_1 = yx - y$, $f_2 = y^2 - x$, dlex sıralamasına göre $x < y$ ve $F = \{f_1, f_2\}$ olsun.

$f \xrightarrow{F} x$ olduğunu gösterelim.

$$y^2x \xrightarrow{f_1} y^2 \xrightarrow{f_2} x$$

$$h_1 = y^2x - \frac{y^2x}{yx}(yx - y) = y^2$$

$$h = y^2 - \frac{y^2}{y^2}(y^2 - x) = x$$

dir.

Tanım 2.1.13: $r \in K[x_1, x_2, \dots, x_n]$ olsun. Eğer $r = 0$ veya $F = \{f_1, f_2, \dots, f_s; f_i \neq 0, 1 \leq i \leq s\}$ için $lm(f_i)$ 'lerden hiçbirisi r 'nin hiçbir monomialini bölmüyorsa r 'ye F 'ye göre indirgenmiş polinomdur denir.

Ayrıca eğer $f \xrightarrow{F} r$ ile indirgenmişse ve r , F 'ye göre bir indirgenmiş polinom ise, r 'ye f 'nin F 'ye göre kalan terimi denir.

Örnek 2.1.7: $Q[x, y]$ 'de $f = y^2x - x$, $f_1 = yx - y$, $f_2 = y^2 - x$, $F = \{f_1, f_2\}$ ve dlex sıralamasına göre $x < y$ olsun.

$lm(f_1) = yx$, $lm(f_2) = y^2$ olup aşağıdaki indirgemeleri düşünelim.

$$f \xrightarrow{f_1} h_1$$

ile

$$f - \frac{y^2x}{yx}(yx - y) = -x + y^2 = h_1$$

elde edilir.

$$f \xrightarrow{f_1} \underbrace{-x + y^2}_{h_1} \xrightarrow{f_2} h_2 = 0$$

ile

$$h_1 - \frac{y^2}{y^2} (y^2 - x) = 0$$

elde edilir. O halde $f - yf_1 - 1.f_2 = 0$ olup

$$f = yf_1 + f_2, \quad f \in \langle f_1, f_2 \rangle \text{ dir.}$$

Sonuç 0 ise $f \in \langle f_1, f_2 \rangle$ dir.

Teorem 2.1.3: $F = \{f_i \mid f_i \neq 0, 1 \leq i \leq s\} \subseteq K[x_1, x_2, \dots, x_n]$ ve $f \in K[x_1, x_2, \dots, x_n]$ verilsin. Bölme algoritması gereğince en az $u_1, u_2, \dots, u_s, r \in K[x_1, x_2, \dots, x_n]$ vardır öyle ki $f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$ dir. Bu durumda

$$lm(f) = \max \left\{ \max_{1 \leq i \leq s} \left(lm(u_i) + lm(f_i) \right), lm(r) \right\} \text{ olup } r \text{ 'nin hiçbir monomialini bölmez.}$$

Örnek 2.1.8: $f = y^2 x - x \in Q[x, y], \quad I = \langle f_1, f_2 \rangle \subseteq Q[x, y],$

$$f_1 = yx - y, f_2 = y^2 - x, F = \{f_1, f_2\} \text{ ve dlex sıralamasına göre } x < y \text{ olsun.}$$

$$f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0 \text{ böylece } f \xrightarrow{F} 0, \text{ indirgemelerine göre } f = yf_1 + f_2 \text{ ve } r = 0 \text{ olduğundan } f \in I = \langle f_1, f_2 \rangle \text{ dir.}$$

Örnek 2.1.9: $f = y^2 x - x \in Q[x, y], \quad F = \{f_1, f_2\}, \quad f_1 = yx - y, f_2 = y^2 - x,$
 $f_1, f_2 \in Q[x, y]$ ve dlex sıralamasına göre $x < y$ olsun.

$$f \xrightarrow{f_1} y^2 \xrightarrow{f_2} x$$

indirgemelerine göre

$$f = yf_1 + 1.f_2 + x, \quad r = x \text{ dir.}$$

Tanım 2.1.14: $K[x_1, x_2, \dots, x_n]$ 'nin bir I ideali tarafından içerilen ve sıfırdan farklı elemanlara sahip bir $G = \{g_1, g_2, \dots, g_t\}$ kümesi verilmiş olsun. Eğer her $f \in I - \{0\}$ ve en az bir $i \in \{1, 2, \dots, t\}$ için $lm(g_i)/lm(f)$ ise G kümesine bir gröbner bazı denir.

Tanım 2.1.15: $S \subseteq K[x_1, x_2, \dots, x_n]$ olsun. $lt(S) = \langle lt(f), f \in S \rangle$ idealine S nin en büyük dereceli terim ideali denir.

Teorem 2.1.4: $G = \{g_1, g_2, \dots, g_t\} \subset K[x_1, x_2, \dots, x_n]$ bir gröbner bazı olması için gerek ve yeter koşul $\langle G \rangle$ ideali içinde bir gröbner bazı olmasıdır.

Tanım 2.1.16: $0 \neq f, g \in K[x_1, x_2, \dots, x_n]$ ve $L = lcm(lm(f), lm(g))$ olsun.

$$S(f, g) = \frac{L}{lt(f)} f - \frac{L}{lt(g)} g$$

polinomuna f ve g 'nin S -polinomu denir.

Örnek 2.1.10: $f = 2yx - y, g = 3y^2 - x, f, g \in Q[x, y]$ dlex sıralamasına göre $x < y$

$$L = y^2 x = lcm(yx, y^2)$$

$$S(f, g) = \frac{y^2 x}{2yx} f - \frac{y^2 x}{3y^2} g = \frac{y}{2} f - \frac{x}{3} g = \frac{-y^2}{2} + \frac{x^2}{3}$$

$$lm\left(\frac{y}{2} f\right) = lm\left(\frac{1}{3} xg\right) = y^2 x$$

dir.

Örnek 2.1.11: $f = y^2 x + 1, f_1 = yx - y, f_2 = y^2 - x, f, f_1, f_2 \in Q[x, y]$

ve dlex sıralamasına göre $x < y$ olsun.

$$f \xrightarrow{f_1} y^2 + 1 = f - y \cdot f_1$$

$$x = L = lcm(\underbrace{lm(f_1)}_{yx}, \underbrace{lm(f_2)}_{y^2}) = y^2 x$$

$$y^2 + 1 + y.f_1 = x^2 + 1 + x.f_2$$

$$-y^2 + x^2 = y.f_1 - x.f_2 = S(f_1, f_2) \in \langle f_1, f_2 \rangle \text{ dir.}$$

Tanım 2.1.17: $G = \{g_1, g_2, \dots, g_t\}$ gröbner bazı olsun. Eğer her i ve $lc(g_i) = 1$ ve her $i \neq j$ için, $lm(g_i), lm(g_j)$ 'yi bölmüyor ise G 'ye minimal gröbner bazı denir.

Tanım 2.1.18: $G = \{g_1, g_2, \dots, g_t\}$ bir gröbner bazı ve herhangi $j \neq i$ için $lm(g_j)/lm(g_i)$ olsun. Eğer her i için $lc(g_i) = 1$ ve $g_i, G - \{g_i\}$ 'ye göre indirgenmişse G 'ye indirgenmiştir denir.

Tanım 2.1.19: $f \in K[x_1, x_2, \dots, x_n]$ ve $f \xrightarrow{G} r$ olsun. r elemanına G 'ye belirtilen sıralama ile f 'nin normal formu denir ve $N_G(f)$ ile gösterilir.

K, k 'nın genişletilmiş cismi olsun. K bir cisim öyle ki $k \subset K$ dir.

$$S \subseteq k[x_1, x_2, \dots, x_n] \text{ ise}$$

$$V_k(S) = \{(a_1, a_2, \dots, a_n) \in K^n \mid f(a_1, \dots, a_n) = 0, \forall f \in S\} \text{ olup}$$

$$\text{eğer } I = \langle f_1, f_2, \dots, f_s \rangle \subseteq k[x_1, x_2, \dots, x_n] \text{ ise}$$

$$V_k(I) = \{(a_1, \dots, a_n) \in K^n \mid f_i(a_1, \dots, a_n) = 0, 1 \leq i \leq s\}$$

$$= V_k(f_1, f_2, \dots, f_s)$$

şeklindedir.

$V \subseteq K^n$ alt kümesi alalım.

$$I(V) \text{ ideali } k[x_1, x_2, \dots, x_n] \text{ de}$$

$$I(V) = \{f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0, \forall (a_1, \dots, a_n) \in V\}$$

şeklinde tanımlanır.

$V_k(S)$ sınıfı, K cismine bağlı olan denklemler sisteminin çözümlerinin bir kümesidir.

Örnek1: $K = R$ alınırsa

$$V_R(x^2 + y^2) = V_R(x, y) = \{(0,0)\} \subseteq R^2 \text{ dir.}$$

$K = C$ için

$$V_C(x^2 + y^2), y = \mp ix, (i = \sqrt{-1}) \text{ doğrularının birleşimidir.}$$

$$V_C(x, y), \{(0,0)\}' \text{ dir.}$$

Örnek2: $f = x^2 + y^2 + 1$ polinomunu alalım.

$$K = R \text{ için } V_R(f) = \emptyset$$

$$K = C \text{ için } V_C(f), \text{ sonsuz sayıda noktaya sahiptir.}$$

$f = x^4 + y^4 + 1$ için de durum benzerdir.

$R[x, y]$ 'nin birçok sonsuz ideali vardır. R^2 deki sınıfları boştur. I ideal olsun.

$$V_R(I) = \emptyset, V_R(I) \subseteq R^2 \text{ dir.}$$

Örnek1 ve Örnek2 bir denklem sisteminin K^n de bazı çözümlere sahip olduğunu gösterir.

Örnek1'de $\langle x^2 + y^2 \rangle$ ve $\langle x, y \rangle$ ideallerinin R 'deki sınıfları aynıdır, fakat esas olarak farklıdır.

Örnek2'de R 'de, C 'ye genişletildiğinde esas olarak farklı idealler farklı sınıflar verir.

Tanım 2.1.20: k 'nın cebirsel kapanışı $\bar{k}$ ile ifade edeceğiz. Eğer her $f \in K[x]$ için $f = 0$ denkleminin K da bir çözümü varsa K cismi cebirsel kapalı bir cisimdir denir. Her k cismi, $\bar{k}$ cebirsel kapalı cismi tarafından kapsanır. Her $\bar{k}$ nın elemanı, $k[x]$ deki sıfırdan farklı bir polinomun köküdür. $\bar{k}$ cismi tektir ve k nın cebirsel kapanışı denir.

Örneğin R 'nin cebirsel kapanışı C dir.

Teorem 2.1.5: (Weak Hilbert Nullstellensatz)

I , $k[x_1, x_2, \dots, x_n]$ 'nin bir ideal olsun. $V_{\bar{k}}(I) = \emptyset$ olması için gerek ve yeter koşul

$I = k[x_1, x_2, \dots, x_n]$ olmasıdır.

Tanım 2.1.21: $I \subset k[x_1, x_2, \dots, x_n]$ bir ideal olsun. $\{f \in k[x_1, x_2, \dots, x_n] \mid e \in N\}$ öyle ki $f^e \in I$ kümesine I 'nin radikali denir ve $\sqrt{I}$ ile gösterilir. $\sqrt{I}$, $k[x_1, x_2, \dots, x_n]$ 'de bir idealdir. Ayrıca her $k \subseteq K$ cismi için $V_K(I) = V_K(\sqrt{I})$ dir.

Teorem 2.1.6: (Strong Hilbert Nullstellensatz)

$I(V_k(I)) = \sqrt{I}$, her $I \subset k[x_1, x_2, \dots, x_n]$ ideali için I ve J idealleri aynı sınıfa sahip olsun.

$V_k(I) = V_k(J)$ olması için gerek ve yeter koşul I ve J nin radikallerinin eşit olmasıdır. ($\sqrt{I} = \sqrt{J}$).

I ve J idealleri esas olarak farklı olması için gerek ve yeter koşul I ve J farklı radikallere sahip olmasıdır.

Örnek1 de $\sqrt{\langle x, y \rangle} = \langle x, y \rangle$ ve $\sqrt{\langle x^2 + y^2 \rangle} = \langle x^2 + y^2 \rangle$

$\langle x^2 + y^2 \rangle$ ve $\langle x, y \rangle$ esas olarak farklı ve C^2 de sınıfları farklıdır.

$I = \langle f_1, f_2, \dots, f_s \rangle, k[x_1, x_2, \dots, x_n]$ 'nin bir ideali olsun ve $G = \{g_1, g_2, \dots, g_t\}$ belirtilmiş bir tam sıralamaya göre I için bir indirgenmiştir.

Tanım 2.1.22: x_1, x_2 kuvvet çarpımları x 'e bağlı y_1, y_2 kuvvet çarpımları y 'e bağlı olsun.

$x_1 y_1 < x_2 y_2 \Leftrightarrow x_1 <_x x_2$ veya $x_1 = x_2$ ve $y_1 <_y y_2$ şeklindeki terim sıralamasına bir eleme sıralaması denir.

Lemma 2.1.2: Eleme sıralaması, bir tam sıralamadır.

Not: $f, g \in k[x_1, x_2, \dots, x_n]$ üzerinde bir terim sıralama olsun.

$f, g \in k[x_1, x_2, \dots, x_n]$, $f, g \neq 0$ için

$(f, g) = d$, f ve g 'nin en büyük ortak böleni olsun. Yani,

- (i) d/f ve d/g
- (ii) eğer h/f ve h/g ise h/d
- (iii) $lc(d) = 1$

dir.

$[f, g] = \ell$, f ve g nin en küçük ortak katı olsun. Yani,

- (i) f/ℓ ve g/ℓ
- (ii) Eğer f/h ve g/h ise ℓ/h
- (iii) $f \cdot g = f, g$

dir.

Tanım 2.1.23: I ve J , $k[x_1, x_2, \dots, x_n]$ de iki ideal olsun.

$J : I = \{g \in k[x_1, x_2, \dots, x_n] \mid gI \subseteq J\}$ kümesi ideal olup bölüm ideali olarak adlandırılır.

2.2. Temel Otomorfizm ve Pik İndirgemesi

$K[t] \times K[t]$, K üzerinde bir değişkenli polinom cebirinin direk çarpımı olsun.

Bu cebirin elemanter dönüşümleri aşağıdaki şekilde tanımlanır.

$$(ET1) \quad (u, v) \longrightarrow (u + \mu.v^k, v), \mu \in K^*, k \geq 2$$

$$(ET2) \quad (u, v) \longrightarrow (u, v + \mu.u^k)$$

$$(ET3) \quad (u, v) \longrightarrow (a_1u + a_2v, b_1u + b_2v); a_1, a_2, b_1, b_2 \in K$$

Tanım 2.2.1: $1 \leq i, j \leq n$ için $\alpha_i, c_{ij} \in K$ olmak üzere $f : x_k \longrightarrow \sum_{i=1}^n c_{ki} x_i + \alpha_k$,

$1 \leq k \leq n$ formundaki bir otomorfizme afin otomorfizm denir.

Tanım 2.2.2: $p \in K[x_1, x_2, \dots, x_n]$ ve $c \in K$ olsun.

$F_c = \{(x_1, x_2, \dots, x_n) \in K^n \mid p(x_1, \dots, x_n) = c\}$ kümesine p 'nin polinom eğrisi (fiberi) denir. Bu kümeyi kısaca $\{p(x_1, \dots, x_n) = c\}$ ile göstereceğiz.

Tanım 2.2.3: Af , $K[x, y]$ 'nin afin otomorfizmlerinin grubu olsun.

$$x \longrightarrow ax + p(y); a, b, c \in K, p(y) \in K[y]$$

$$y \longrightarrow by + c$$

formundaki otomorfizmlere üst üçgensel otomorfizmlerin grubu denir ve $\ddot{U}\ddot{U}$ ile gösterilir.

$$x \longrightarrow ax + b$$

$$y \longrightarrow by + p(x)$$

formundaki otomorfizmlere alt üçgensel otomorfizmlerin grubu denir ve $A\ddot{U}$ ile gösterilir.

$$x \longrightarrow ax + p(y); a, b, c, d \in K, p(y) \in K[y]$$

$$y \longrightarrow by + cx + d$$

formundaki otomorfizmlere twisted üst üçgensel otomorfizmlerin grubunu denir ve $T\ddot{U}\ddot{U}$ ile gösterilir.

$$x \longrightarrow ax + by + c$$

$$y \longrightarrow d.y + p(x)$$

formundaki otomorfizmlere twisted alt üçgensel otomorfizmlerin grubunu denir ve $TA\ddot{U}$ ile gösterilir.

$$T\ddot{U}\ddot{U} \cap TA\ddot{U} = Af \text{ dir.}$$

3. GRÖBNER BAZININ TEMEL UYGULAMALARI

Bu kısımda Gröbner bazı ile ilgili temel sonuçlar incelenerek çeşitli örnekler verilecektir.

3.1.Gröbner Bazı

Teorem 3.1.1: $0 \neq I \Delta K[x_1, x_2, \dots, x_n]$ olsun.

$G = \{g_1, g_2, \dots, g_t\} \subseteq I$ olmak üzere aşağıdakiler birbirlerine denktir.

(i) G bir gröbner bazıdır.

(ii) Her $f \in I$ için gerek ve yeter koşul $f \xrightarrow{G} 0$ olmasıdır.

(iii) Her $f \in I$ için gerek ve yeter koşul $f = \sum_{i=1}^t h_i g_i$ öyle ki

$lm(f) = \max \left\{ lm(h_i).lm(g_i) \right\}_{1 \leq i \leq t}$ olmasıdır.

(iv) $lt(I) = lt(G)$

dir.

İspat: G bir gröbner bazı ve $f \in I$ olsun.

$f \xrightarrow{G} 0$ açıktır.

$f \xrightarrow{g_1} r, f = \underbrace{u_1 g_1}_{\in I} + r \in I, r \in I$ ve $r = 0$ olur.

$f \xrightarrow{G} 0$ olsun.

$f = \underbrace{u_1 g_1}_{\in I} + \underbrace{u_2 g_2}_{\in I} + \dots + \underbrace{u_t g_t}_{\in I} + 0$

$f \in G = \{g_1, g_2, \dots, g_t\} \subseteq I$ ve böylece $f \in I$ olur.

Her $f \in I$ için gerek ve yeter koşul $f = \sum_{i=1}^t h_i g_i$ olsun.

$lt(G) = \langle lt(g), g \in G, g \in I \rangle \subseteq lt(I)$ olur.

$lt(f) \in lt(I)$ alalım.

$$lt(f) = \max \left\{ lt(h_i), lt(g_i) \right\}_{1 \leq i \leq t} = lt(h_{j_0}) \underbrace{lt(g_{j_0})}_{\in lt(G)} \in lt(G)$$

$$lt(I) = lt(G)$$

dir.

$lt(I) = lt(G)$ olsun. $f \in I$ alalım.

$$lt(f) \in lt(I) = lt(G)$$

$lt(f) = u_1 lt(g_1) + u_2 lt(g_2) + \dots + u_t lt(g_t)$ olacak şekilde $u_i \in K[x_1, x_2, \dots, x_n]$ vardır.

$$lt(f) = \underbrace{u_1}_{\frac{lm(g_1)}{lc(g_1)}} lt(g_1) + \underbrace{u_2}_{\frac{lm(g_2)}{lc(g_2)}} lt(g_2) + \dots + \underbrace{u_t}_{\frac{lm(g_t)}{lc(g_t)}} lt(g_t)$$

$$lm(f) = u'_1 lm(g_1) + \dots + u'_t lm(g_t)$$

En az bir i_0 için $lm(g_{i_0})/lm(f)$ ise G gröbner bazıdır.

Sonuç 3.1.1: $G = \{g_1, g_2, \dots, g_t\}$, I ideali için bir gröbner bazı ise $I = \langle G \rangle$ dir.

İspat: $f \in I$ alalım. Bölme algoritması uygulayalım.

$f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t + r$ öyle ki hiçbir $lm(g_i)$, r monomialini bölmez.

$r = 0$ ise ispat tanımlanır.

$r \neq 0$ olsun. $r \in I$ dir. G gröbner bazı olduğundan en az bir j için $lm(g_j)/lm(r)$

olur. Böylece $r = 0$ olur. Bu da kabulümüzle çelişir. O zaman $I = \langle G \rangle$ olur.

Lemma 3.1.1: $I = \langle S \rangle$ olacak şekilde $0 \notin S$ ve $f \in K[x_1, x_2, \dots, x_n]$ olsun. $f \in I$ için

gerek ve yeter koşul f deki her m monomiali ve en az bir $y \in S$ için y/m dir.

Ayrıca $I = \langle S_0 \rangle$ olacak şekilde S 'nin bir sonlu alt kümesi vardır.

İspat: $I \Delta K[x_1, x_2, \dots, x_n]$ olup en az $f_1, f_2, \dots, f_t \in K[x_1, x_2, \dots, x_n]$ için

$I = \langle f_1, f_2, \dots, f_t \rangle$ dir. $K[x_1, x_2, \dots, x_n]$ bir noetherian halkasıdır.

$I = \langle S \rangle$ ise her $f \in I$ için f 'nin terimleri S 'nin en az bir elemanı tarafından bölünür. S sonlu ise ispat tamamlanmış olur.

Şimdi S 'nin sonlu olmadığını kabul edelim. O zaman $f_i \in I$ olup $s_1/f_1, s_2/f_2, \dots, s_t/f_t$ olacak şekilde $s_1, s_2, \dots, s_t \in S$ bulabiliriz.

$S_0 = \{s_1, s_2, \dots, s_t\}$ alalım. $I = \langle S_0 \rangle$ olsun.

$f \in I$ ise $f = u_1 f_1 + u_2 f_2 + \dots + u_t f_t$ dir.

Aynı zamanda $f = u'_1 s_1 + u'_2 s_2 + \dots + u'_t s_t$ dir. Buradan

$f \in \langle s_1, s_2, \dots, s_t \rangle = \langle S_0 \rangle$ olup $I = \langle S_0 \rangle$ dir.

Sonuç 3.1.2: $K[x_1, x_2, \dots, x_n]$ 'nin her I ideali için en az bir sonlu gröbner bazı vardır.

İspat: $lt(I) = \langle lt(f); f \in I \rangle$

Lemma 3.1.1 ile $S_0 = \{lt(g_1), lt(g_2), \dots, lt(g_t)\}$ olacak şekilde Lemma 3.1.1.deki özellikleri sağlayan bir S_0 mevcuttur.

$lt(I) = \langle lt(g_1), lt(g_2), \dots, lt(g_k) \rangle$, $G = \{g_1, g_2, \dots, g_t\}$ alırsak $lt(G) = lt(I)$ olur.

Teorem 3.1.1 den G gröbner bazıdır.

Önerme 3.1.1: $K[x_1, x_2, \dots, x_n]$ 'nın her $I \neq 0$ ideali bir gröbner baza sahiptir.

İspat: $lt(I) = \langle lt(f); f \in I \rangle$

$lt(I), \{lt(g_1), lt(g_2), \dots, lt(g_t)\}$ formunda sonlu üreteçli bir kümeye sahiptir.

$g_1, g_2, \dots, g_t \in I$ dir. $G = \{g_1, g_2, \dots, g_t\}$ ise $lt(G) = lt(I)$ dir.

$lt(G) = lt(I)$ ise G, I için bir gröbner bazıdır.

Teorem 3.1.2: $G = \{g_1, g_2, \dots, g_t\} \subset K[x_1, x_2, \dots, x_n]$, G bir gröbner bazı olsun.
 $f \in K[x_1, x_2, \dots, x_n]$ için G ile bölümünden kalan terimi tektir.

İspat: G , bir gröbner bazı olsun.

$f \xrightarrow{G} r_1$ ve $f \xrightarrow{G} r_2$ olacak şekilde $r_1 \neq r_2$ olsun.

Bölme algoritmasından $f = u_1 g_1 + u_2 g_2 + \dots + u_t g_t + r_1$ ve

$f = v_1 g_1 + v_2 g_2 + \dots + v_t g_t + r_2$ olacak şekilde yazılır. Ayrıca $lm(g_i)$, r_1 ve r_2 'nin monomiallerini bölmesin.

$u_i, v_i \in K[x_1, x_2, \dots, x_n]$ olsun.

$0 = w_1 g_1 + w_2 g_2 + \dots + w_t g_t + (r_1 - r_2)$ dir.

$w_i = u_i - v_i$ ve $r_1 - r_2 \in I$ olacak şekilde en az bir g_j için $lm(g_j) \mid lm(r_1 - r_2)$ dir.

$r_1 - r_2 = 0$ ise $r_1 = r_2$ dir.

Örnek 3.1.1: $f = y^2 x - x \in Q[x, y]$, $f_1 = yx - y$, $f_2 = y^2 - x$, $F = \{f_1, f_2\}$ ve dlex sıralamasına göre $y > x$ olsun. Uygulanan indirgemelere göre

$$f \xrightarrow{f_1} y^2 - x \xrightarrow{f_2} 0 \text{ ve } f \xrightarrow{f_2} x^2 - x \quad \text{dir.}$$

$$x^2 = lm(x^2 - x), \quad lm(f_1) = xy, \quad lm(f_2) = y^2.$$

Böylece $lm(f_1)$ veya $lm(f_2)$, $lm(x^2 - x)$ i bölmez. O halde

$$f \xrightarrow{F} 0, \quad f = y \cdot f_1 + f_2, \quad f \in \langle f_1, f_2 \rangle$$

olup $F = \{f_1, f_2\}$ bir gröbner bazı değildir.

Örnek 3.1.2: $g_1 = z + x$, $g_2 = y - x \in Q[x, y, z]$, $G = \{g_1, g_2\}$ ve $I = \langle g_1, g_2 \rangle$

lex sıralamasına göre $x < y < z$ olsun.

$G = \{g_1, g_2\}$ nin gröbner bazı olup olmadığını inceleyelim.

Çözüm: $lm(g_1) = z$, $lm(g_2) = y$, G 'nin gröbner bazı olması için her $f \in \langle G \rangle$ için ya $lm(g_1) = z/lm(f)$ yada $lm(g_2) = y/lm(f)$ olmalıdır.

$x/lm(f)$ ise f 'de sıralamadan dolayı y ve z 'li terimler yoktur.

$lm(g_1)$ ve $lm(g_2)$, $lm(f)$ 'yi bölmesin. O halde en az bir $k \in \mathbb{N}$ için $lm(f) = x^k$ dir.

$f \in \langle g_1, g_2 \rangle$ olduğundan en az bir $u_i \in Q[x, y, z]$ için $f = u_1 g_1 + u_2 g_2$ dir. Buradan

$f = u_1(z + x) + u_2(y - x)$ yazarız. Böylece

$f = u_1(x, y, z)(z + x) + u_2(x, y, z)(y - x)$ olur.

y yerine x yazalım.

$f = u_1(x, y, z)(z + x) + 0 = u_1(x, y, z).z + u_1(x, y, z)x$ olup

$f = 0$ veya $f \neq 0$ ise $lm(g_1)/lm(f)$ yada $lm(g_2)/lm(f)$ dir. O halde G , bir gröbner bazıdır.

3.2. S-Polinomları

Bu kısımda S -polinomu ile ilgili temel sonuçlar incelenerek çeşitli örnekler verilecektir.

$f, g \in K[x_1, x_2, \dots, x_n]$ ve $L = lcm(lm(f), lm(g))$ olsun. f ve g 'nin S -polinomu

$$S(f, g) = \frac{L}{It(f)} f - \frac{L}{It(g)} g \quad (3.1)$$

olarak tanımlanır.

Lemma 3.2.1: $f_1, f_2, \dots, f_s \in K[x_1, x_2, \dots, x_n]$

Her $i = 1, 2, \dots, s$ için $lm(f_i) = x \neq 0$

$$f = \sum_{i=1}^s c_i f_i, \quad c_i \in K$$

Eğer $lm(f) < x$ ise f , $1 \leq i < j \leq s$ olmak üzere $S(f_i, f_j)$ 'nin bir lineer birleşimidir.

İspat: $f_i = a_i x + z$, $a_i \in K$ ve z daha düşük dereceli terimleri içeren bir polinom olsun.

Hipotezden $lm(f) < x$ olmalı ve $\sum_{i=1}^s c_i a_i = 0$, $c_i \in K$ dir.

$$S(f_i, f_j) = \frac{1}{a_i} f_i - \frac{1}{a_j} f_j \text{ alalım.}$$

$$lm(f_i) = lm(f_j) = x \text{ dir.}$$

$$f = c_1 f_1 + c_2 f_2 + \dots + c_s f_s = c_1 a_1 \left(\frac{1}{a_1} f_1 \right) + \dots + c_s a_s \left(\frac{1}{a_s} f_s \right) \text{ dir.}$$

$$f = c_1 a_1 \left(\frac{1}{a_1} f_1 - \frac{1}{a_2} f_2 \right) + (c_1 a_1 + c_2 a_2) \left(\frac{1}{a_2} f_2 - \frac{1}{a_3} f_3 \right) + \dots +$$

$$(c_1 a_1 + \dots + c_{s-1} a_{s-1}) \left(\frac{1}{a_{s-1}} f_{s-1} - \frac{1}{a_s} f_s \right) + (c_1 a_1 + \dots + c_s a_s) \frac{1}{a_s} f_s$$

Böylece f , $S(f_i, f_j)$ 'nin lineer birleşimi olarak

$$f = c_1 a_1 S(f_1, f_2) + (c_1 a_1 + c_2 a_2) S(f_2, f_3) + \dots + (c_1 a_1 + \dots + c_{s-1} a_{s-1}) S(f_{s-1}, f_s)$$

şeklinde yazılır.

Teorem 3.2.1: (Buchberger)

$G = \{g_1, g_2, \dots, g_t\}$ sıfırdan farklı $K[x_1, x_2, \dots, x_n]$ deki polinomlar kümesi olsun.

G 'nin, $I = \langle g_1, g_2, \dots, g_t \rangle$ ideali için bir gröbner bazı olması için gerek ve yeter koşul her $i \neq j$ için $S(g_i, g_j) \xrightarrow{G} 0$ olmasıdır.

İspat: $G = \{g_1, g_2, \dots, g_t\}$, $I = \langle g_1, g_2, \dots, g_t \rangle$ için bir gröbner bazı olsun. Her $i \neq j$ için $S(g_i, g_j) \in I$ 'dir. Teorem 3.1.1'den her $f \in I$ olması için gerek ve yeter koşul $f \xrightarrow{G} 0$ ve G , gröbner bazı olmasıdır.

$S(g_i, g_j) \xrightarrow{G} 0$ dir.

Şimdi $i \neq j$ olmak üzere $S(g_i, g_j) \xrightarrow{G} 0$ olsun. G 'nin I için bir gröbner bazı olduğunu göstermek için $f \in I$ için $X = \max_{1 \leq i \leq t} (lm(h_i), lm(g_i))$ olduğunu göstermeliyiz.

$lm(f) = X$ ise Teorem 3.1.1 den G , bir gröbner bazıdır. Aksi takdirde $lm(f) < X$ dir.

$S = \{i | lm(h_i), lm(g_i) = X\}$, $i \in S$, $h_i = c_i X_i + \text{diğer terimler}$

$lm(g) = X_1 g_1$, $\underbrace{lm(h_1)}_{X_1} \underbrace{lm(g_1)}_{< X} = X$ dir.

$g = \sum_{i \in S} c_i X_i g_i$ olsun. Her $i \in S$ için

$lm(X_i g_i) = X$ dir. Fakat $lm(g) < X$ olup Lemma 3.2.1 den

$$g = \sum d_{ij} S(X_i g_i, X_j g_j), d_{ij} \in K \text{ dir.}$$

$X = lcm(lm(X_i g_i), lm(X_j g_j))$ alalım. Buradan

$$\begin{aligned} S(X_i g_i, X_j g_j) &= \frac{X}{It(X_i g_i)} X_i g_i - \frac{X}{It(X_j g_j)} X_j g_j \\ &= \frac{X}{It(g_i)} g_i - \frac{X}{It(g_j)} g_j \\ &= \frac{X}{X_{ij}} S(g_i, g_j) \text{ olur. (Burada } X_{ij} = lcm(lm(g_i), lm(g_j)) \text{ dir.)} \end{aligned}$$

Böylece $S(g_i, g_j) \xrightarrow{G} 0$ olduğundan $S(X_i g_i, X_j g_j) \xrightarrow{G} 0$ olur.

$$\max_{1 \leq v \leq t} (Im(h_{ijv}), Im(g_v)) = Im(S(X_i g_i, X_j g_j)) < \max(Im(X_i g_i), Im(X_j g_j)) = X$$

$$f = \sum_{i=1}^t h_i g_i$$

$$\max_{1 \leq v \leq t} (Im(h_i), Im(g_i)) < X \text{ dir.}$$

Sonuç 3.2.1: $G = \{g_1, g_2, \dots, g_t\}$ ve $1 \leq i \leq t$ için $g_i \neq 0$

G , bir gröbner bazı olması için gerek ve yeter koşul $1 \leq i, j \leq t$ olmak üzere her $i \neq j$ için

$$S(g_i, g_j) = \sum_{v=1}^t h_{ijv} g_v \text{ ve}$$

$$Im(S(g_i, g_j)) = \max_{1 \leq v \leq t} (Im(h_{ijv}), Im(g_v))$$

olmasıdır.

İspat: [2] de verilmiştir.

Örnek 3.2.2: $f_1 = xy - x$, $f_2 = x^2 - y \in Q[x, y]$, $F = \{f_1, f_2\}$ ve dlex sıralamasına göre $x < y$ olsun. Gröbner bazını bulalım.

$$S(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 \xrightarrow{F} y^2 - y, f_3 = y^2 - y$$

$S(f_1, f_2)$ polinomu F 'ye göre indirgenmesi sonucunda f_3 polinomu elde edilir.

$$F' = \{f_1, f_2, f_3\} \text{ olsun.}$$

$$S(f_1, f_2) \xrightarrow{F'} 0$$

$$S(f_1, f_3) = y \cdot f_1 - x \cdot f_3 \xrightarrow{F'} 0$$

$$S(f_2, f_3) = y^2 f_2 - x^2 f_3 = -y^3 + x^2 y \xrightarrow{F'} x^2 y - y^2 \xrightarrow{F'} 0$$

indirgemelerini uygulayalım. Böylece $F' = \{f_1, f_2, f_3\}$, bir gröbner bazıdır.

Örnek 3.2.3: $f_1 = x^2 + y^2 + 1$, $f_2 = x^2 y + 2xy + x \in Z_5[x, y]$ alalım.

$F = \{f_1, f_2\}$ ve lex sıralamasına göre $x > y$ olsun. $S(f_1, f_2)$ polinomu F 'ye göre indirgenmesi sonucunda f_3 polinomu elde edilir.

$$S(f_1, f_2) = y \cdot f_1 - f_2 = 3xy + 4x + y^3 + y, f_3 = 3xy + 4x + y^3 + y$$

$$F' = \{f_1, f_2, f_3\} \text{ olsun.}$$

$$S(f_1, f_2) \xrightarrow{F'} 0$$

$$S(f_1, f_3) \xrightarrow{F'} 4y^5 + 3y^4 + y^2 + y + 3, f_4 = 4y^5 + 3y^4 + y^2 + y + 3$$

$S(f_1, f_3)$ polinomu F 'ye göre indirgenmesi sonucunda f_4 polinomu elde edilir.

$$F'' = \{f_1, f_2, f_3, f_4\} \text{ olsun.}$$

$$S(f_1, f_4) \xrightarrow{F''} 0$$

$$S(f_2, f_4) \xrightarrow{F''} 0$$

$$S(f_3, f_4) \xrightarrow{F''} 0$$

$$S(f_2, f_3) \xrightarrow{F''} 0$$

indirgemeleri sonucunda $F'' = \{f_1, f_2, f_3, f_4\}$, bir gröbner bazıdır.

Lemma 3.2.2: $G = \{g_1, g_2, \dots, g_t\}$, I 'nın bir gröbner bazı olsun. Eğer $lm(g_2)/lm(g_1)$ ise $\{g_2, g_3, \dots, g_t\}$ de I 'nın bir gröbner bazıdır.

İspat: $f \in I$ ve $lm(g_1)/lm(f)$ olsun.

Eğer $lm(g_2)/lm(g_1)$ ise $lm(g_2)/lm(f)$ 'dir. $lm(f)$ 'yi bölen en az bir $lm(g_2)$ olduğu için $\{g_2, g_3, \dots, g_t\}$ bir gröbner bazıdır.

Önerme 3.2.1: $G = \{g_1, g_2, \dots, g_t\}$ ve $F = \{f_1, f_2, \dots, f_s\}$ I için iki minimal gröbner bazı ise $s = t$ ve sonra gerekiyorsa tekrar numaralandırıldıktan sonra her $i = 1, 2, \dots, t$ için $lm(f_i) = lm(g_i)$ olur.

İspat: F ve G , I için iki gröbner bazıdır. En az bir i için $lm(g_i)/lm(f_1)$ bu durum tekrar edilir. $f_1 \in I$ olup F , I için bir gröbner bazıdır. O zaman en az bir j için $lm(f_j)/lm(g_1)$ dir.

Sonuç olarak $lm(f_j)/lm(f_1)$ dir. Bu durumda $j = 1$ olur ve F , bir gröbner bazı olduğundan $lm(f_1) = lm(g_1)$ dir. Böyle devam ederek

$$lm(f_2) = lm(g_2)$$

⋮

$$lm(f_t) = lm(g_t) \text{ dir.}$$

$G = \{g_1, g_2, \dots, g_t\}$ gröbner bazı olsun. Eğer her i ve $lc(g_i) = 1$ ve her $i \neq j$ için, $lm(g_i)$, $lm(g_j)$ 'yi bölmüyor ise G 'ye minimal gröbner bazı denir.

Önerme 3.2.2. G , I için bir minimal gröbner bazı olsun.

$$g_1 \xrightarrow{H_1} h_1 \quad \text{öyle ki } H_1 = G - \{g_1\}$$

$$g_2 \xrightarrow{H_2} h_2 \quad \text{öyle ki } H_2 = \{h_1, g_3, \dots, g_t\}$$

$$g_3 \xrightarrow{H_3} h_3 \quad \text{öyle ki } H_3 = \{h_1, h_2, g_4, \dots, g_t\}$$

$\vdots$

$$g_i \xrightarrow{H_i} h_i \quad \text{öyle ki } H_i = \{h_1, h_2, \dots, h_{i-1}\}$$

Böylece $H = \{h_1, h_2, \dots, h_t\}$ indirgenmiş bir gröbner bazıdır.

İspat: $g_1 \xrightarrow{H_1} h_1$,

$$g_1 = u_2 g_2 + u_3 g_3 + \dots + u_t g_t + h_1 \text{ ve}$$

$$lm(g_1) = \max_{2 \leq i \leq t} \{lm(u_i), lm(g_i), lm(h_1)\} \text{ ve } lm(g_1) \neq lm(h_1) \text{ olsun.}$$

En az bir $i_0 \in \{2, 3, \dots, t\}$ için $lm(g_1) = lm(u_{i_0})lm(g_{i_0})$ dır.

Böylece $lm(g_{i_0})/lm(g_1)$ olur. G , minimal olduğundan çelişki elde edilir.

$$lm(g_1) = lm(h_1) \text{ ve } lm(g_2) = lm(h_2) \text{ dir.}$$

Her i için $lm(g_i) = lm(h_i)$ dir.

O halde $H = \{h_1, h_2, \dots, h_t\}$ indirgenmiş bir gröbner bazıdır.

Teorem 3.2.2: (Buchberger Teoremi)

Bir tam sıralama ele alalım. Sıfırdan farklı her $I \neq 0$ ideali alınan bu sıralamaya göre tek bir indirgenmiş gröbner baza sahiptir.

İspat: Her ideal bir gröbner baza sahiptir. I bir ideal ve $G = \{g_1, g_2, \dots, g_t\}$ $H = \{h_1, h_2, \dots, h_t\}$, I için indirgenmiş iki gröbner bazı olsun.

Önerme 3.2.1. den G ve H minimal olup her i için $lm(g_i) = lm(h_i)$ olur. H ve G , minimal gröbner bazı olduklarından elemanları aynı sayılardadır ve i için $lm(g_i) = lm(h_i)$ dir.

Eğer $g_i \neq h_i$ ise $g_i - h_i \neq 0$ ve $g_i - h_i \in I$ dır.

H , gröbner bazı olduğundan en az bir j için $lm(h_j)/lm(g_i - h_i)$ ve en az bir j için $lm(g_j)/lm(g_i - h_i)$ olur.

$i \neq j$ için $lm(g_i - h_i) < lm(h_i)$ dir. Fakat $lm(g_j) = lm(h_j)$, g_i veya h_i 'nin bir terimini böler. G ve H minimal olduğundan $i = j$ olmalıdır. Bu da bir çelişkidir. G ve H indirgenmiş gröbner bazıdır. Böylece $g_i = h_i$ dir.

Örnek 3.2.4: $f_1 = y^2 + yx + x^2$, $f_2 = y + x$, $f_3 = y \in Q[x, y]$ ve

lex sıralamasına göre $y > x$ olsun. $I = \langle f_1, f_2, f_3 \rangle$ idealinin gröbner bazı $\{f_1, f_2, f_3, f_4, f_5\}$ 'dir. $S(f_1, f_2)$, $S(f_1, f_3)$, $S(f_2, f_3)$ polinomları $F = \{f_1, f_2, f_3\}$ 'e göre indirgenmeleri sonucunda f_4 ve f_5 elde edilir.

$$f_4 = x^2, f_5 = x$$

$\{f_3, f_5\}$ ve $\{f_2, f_5\}$, I ideali için minimal gröbner bazıdır.

$f_3 = y$ ve $f_5 = x$ ve $\{f_3, f_5\}$, I için indirgenmiş bir gröbner bazıdır.

$$f_2 = y + x, f_5 = x$$

$f_2 \xrightarrow{f_5} y$ olduğundan $\{f_2, f_5\}$, I için indirgenmiş bir gröbner bazı değildir. O zaman $\{f_3, f_5\}$, I için tek indirgenmiş gröbner bazıdır.

3.3. Gröbner Bazı İle İlgili Temel Uygulamalar

$$F = \{f_1, f_2, \dots, f_s\} \text{ ve } G = \{g_1, g_2, \dots, g_t\}$$

$I = \langle f_1, f_2, \dots, f_s \rangle$ için belirtilen bir tam sıralamaya göre bir gröbner baz olsun.

$f \in I$ olması için gerek ve yeter koşul $f \xrightarrow{G} 0$ olmasıdır. Burada

$$f \in I, \quad f = u_1 g_1 + \dots + u_i g_i, \quad 1 \leq i \leq t, \quad u_i \in K \text{ dır.}$$

Buchberger'nin algoritmasından yararlanarak $f \in I$ polinomu için $v_i \in K$ olmak üzere $f = v_1 f_1 + v_2 f_2 + \dots + v_s f_s$ şeklinde yazılır. $m, t \times s$ tipinde bir matris olsun. O zaman

$$\begin{bmatrix} g_1 \\ g_2 \\ . \\ . \\ g_t \end{bmatrix} = m \begin{bmatrix} f_1 \\ f_2 \\ . \\ . \\ f_s \end{bmatrix}$$

şeklindedir.

Örnek 3.3.1: $K = Q$ alalım. $f_1 = x^2 y - y + x$, $f_2 = xy^2 - x$, $F = \{f_1, f_2\}$ ve $I = \langle f_1, f_2 \rangle$ olsun. $x < y$ olmak üzere deglex sıralamasına göre gröbner bazını bulalım.

$$S(f_1, f_2) = yf_1 - xf_2 = -y^2 + xy + x^2 \text{ olduğundan}$$

$$f_3 = -y^2 + xy + x^2 \text{ elde edilir. Böylece } F' = \{f_1, f_2, f_3\} \text{ olur. İndirgemelerle}$$

$$S(f_1, f_3) = yf_1 + x^2 f_3 = x^3 y + x^4 - y^2 + xy$$

$$\xrightarrow{f_1} x^4 - y^2 + 2xy - x^2$$

$$\xrightarrow{f_3} x^4 + xy - 2x^2$$

$$f_4 = x^4 + xy - 2x^2$$

$$F'' = \{f_1, f_2, f_3, f_4\} \text{ elde edilir. İndirgemelere devam edersek bu defa}$$

$$\begin{aligned} f_4 &= (yf_1 + x^2 f_3) - xf_1 - f_3 \\ &= (x^2 y - x)f_1 + (-x^3 + x)f_3 \end{aligned}$$

$$S(f_2, f_3) = f_2 + xf_3 = x^2 y + x^3 - x \xrightarrow{f_1} x^3 + y - 2x$$

$$f_5 = x^3 + y - 2x \text{ elde edilir ve}$$

$$(f_2 + xf_3) - f_1 = (xy - 1)f_1 + (-x^2 + 1)f_2$$

$F''' = \{f_1, f_2, f_3, f_4, f_5\}$, I için bir gröbner bazı olur.

$lt(f_3)$, $lt(f_2)$ 'i böler ve $lt(f_5)$, $lt(f_4)$ 'i böldüğünden $\{f_1, f_3, f_5\}$ 'de I için gröbner bazıdır. Bunu matris formunda yazarsak

$$\begin{bmatrix} f_1 \\ f_2 \\ f_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ y & -x \\ xy-1 & -x^2+1 \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} \text{ elde edilir.}$$

Şimdi bir $f \in I$ alalım. İndirgemeler uygulanırsa

$$f = x^4 y - 2x^5 + 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^2 y + 2x^3 - y + 2x$$

$$f \xrightarrow{x^2 f_1} -2x^5 + 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 2x^2 y + x^3 - y + 2x$$

$$\xrightarrow{-2x^2 f_5} 2x^2 y^2 - 2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 - y + 2x$$

$$\xrightarrow{2yf_1} -2x^3 y - 2x^4 - 2y^3 + 4xy^2 - 3x^3 + 2y^2 - 2xy - y + 2x$$

$$\xrightarrow{-2yf_5} -2x^4 - 2y^3 + 4xy^2 - 3x^3 + 4y^2 - 6xy - y + 2x$$

$$\xrightarrow{2yf_3} 2xy^2 - 2x^2 y - 3x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$

$$\xrightarrow{-2xf_3} -x^3 + 4y^2 - 4xy - 4x^2 - y + 2x$$

$$\xrightarrow{-1f_5} 4y^2 - 4xy - 4x^2$$

$$\xrightarrow{-4f_3} 0$$

$$= (x^2 + 2y)f_1 + (2y - 2x - 4)f_3 + (-2x^2 - 2y - 2x - 1)f_5$$

$$= (x^2 + 2y)f_1 + (2y - 2x - 4)f_3 + (-2x^2 - 2y - 2x - 1)f_5$$

$$\begin{aligned} f &= (x^2 + 2y)f_1 + (2y - 2x - 4)(yf_1 - xf_2) + \\ &(-2x^2 - 2y - 2x - 1)((xy - 1)f_1 + (-x^2 + 1)f_2) \end{aligned}$$

$$= (-2x^3 - 2xy^2 - 2x^2y + 2y^2 - 3xy + 3x^2 + 2x + 1)f_1 + (2x^4 + 2x^2y + 2x^3 - 2xy + x^2 - 2y + 2x - 1)f_2$$

şeklinde olur.

Örnek 3.3.2: $K = Z_5$ alalım. $f_1 = x^2 + y^2 + 1$, $f_2 = x^2y + 2xy + x$

$$I = \langle f_1, f_2 \rangle \subseteq Z_5[x, y]$$

$x > y$ olmak üzere lex sıralamasına göre I nin gröbner bazını bulalım.

$$g_1 = f_1$$

$$g_2 = 2f_3 = xy + 3x + 2y^3 + 2y,$$

$$g_3 = 4f_4 = y^5 + 2y^4 + 4y^2 + 4y + 2 \text{ olmak üzere}$$

$\{g_1, g_2, g_3\}$, I için gröbner bazıdır.

$$g_2 = 2yf_1 + 3f_2$$

$$g_3 = 4(y + 3)g_1 + 2(3x + 4y^2 + 3y)g_2$$

$$= (2xy + y^3 + 2y^2 + 4y + 2)f_1 + (3x + 4y^2 + 3y)f_2$$

$$\begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 2y & 3 \\ 2xy + y^3 + 2y^2 + 4y + 2 & 3x + 4y^2 + 3y \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix}$$

I ve J , $K[x_1, x_2, \dots, x_n]$ nin iki ideali olsun.

Buchberger teoreminin bir sonucu olarak I ve J ideallerinin denk olması için gerek ve yeter koşul I ve J nin aynı indirgenmiş gröbner bazına sahip olmasıdır.

Özellikle $I = K[x_1, x_2, \dots, x_n]$ olması için gerek ve yeter koşul I 'nin indirgenmiş gröbner bazının $\{1\}$ olmasıdır.

Önerme 3.3.1: $f, g \in K[x_1, x_2, \dots, x_n]$ olsun.

$f \equiv g \pmod{I}$ olması için gerek ve yeter koşul $N_G(f) = N_G(g)$ olmasıdır.

$\{N_G(f) \mid f \in K[x_1, x_2, \dots, x_n]\}$ kümesi, $K[x_1, x_2, \dots, x_n]/I$ için koset temsilcilerinin bir kümesidir. N_G ,

$N_G : K[x_1, x_2, \dots, x_n] \longrightarrow K[x_1, x_2, \dots, x_n]$ şeklinde bir k -lineer fonksiyondur.

İspat: Bölme algoritmasından $q \in I$ olmak üzere

$f = q + N_G(f)$ dir. Buradan $f - N_G(f) = q \in I$ olur. Böylece

$f + I = N_G(f) + I \in K[x_1, x_2, \dots, x_n]/I$ şeklindedir.

$c_1, c_2 \in k$, $f_1, f_2 \in K[x_1, \dots, x_n]$ için

$c_1(f_1 - N_G(f_1)) + c_2(f_2 - N_G(f_2)) \in I$ olup

$c_1 f_1 + c_2 f_2 - (c_1 N_G(f_1) + c_2 N_G(f_2)) \in I$ dir.

Böylece $c_1 N_G(f_1) + c_2 N_G(f_2)$, G 'e göre belirlenmiş sıralama ile indirgenmiştir.

$N_G(c_1 f_1 + c_2 f_2) = c_1 N_G(f_1) + c_2 N_G(f_2)$ olup N_G , k -lineerdir.

$f \equiv g \pmod{I}$ olması için gerek ve yeter koşul $q \in I$ ve $f = q + g$ olmasıdır.

Böylece

$$N_G(f) = N_G(q + g) \underset{k\text{-lineer}}{=} N_G(q) + N_G(g)$$

$q \in I$ olduğundan $N_G(q) = 0$ dir.

$N_G(f) = N_G(g)$ olur.

$$f - g = q \in I$$

$(f - N_G(f)) - (g - N_G(g)) \in I$ ve $f \equiv g \pmod{I}$ dir.

Örnek 3.3.3: Örnek 3.3.1'e geri dönersek

$$x^3 \xrightarrow{f_5 = x^3 + y - 2x} -y + 2x$$

$-y + 2x$, indirgenmiştir.

$$N_G(x^3) = -y + 2x$$

$$x^2y + y \xrightarrow{f_1 = x^2y - y + x} 2y - x$$

$2y - x$, indirgenmiştir.

$$N_G(x^2y + y) = 2y - x \text{ dir.}$$

$$N_G(x^3) \neq N_G(x^2y + y) \text{ olduğundan}$$

$$x^3 \not\equiv x^2y + y \pmod{I}$$

dir.

Önerme 3.3.2: $G = \{g_1, g_2, \dots, g_t\} \subset K[x_1, x_2, \dots, x_n]$ ve $x \in T^n$ olsun. Her $i = 1, 2, \dots, t$ için $lm(g_i)$, x 'i bölmüyorsa bütün $x \in T^n$ kuvvet çarpımlarının kosetlerinden meydana gelen $K[x_1, x_2, \dots, x_n]_I$ kümesi, k -vektör uzayı için bir bazıdır.

İspat: $f \in K[x_1, x_2, \dots, x_n]$ olsun. O zaman

$$f + I = N_G(f) + I \in K[x_1, x_2, \dots, x_n]_I \text{ dir.}$$

$N_G(f)$, $x \in T^n$ kuvvet çarpımlarının bir lineer birleşimidir. Kuvvet çarpımlarının kosetleri lineer bağımsızdır.

Örnek 3.3.4: Örnek 3.3.1 dlex sıralamasına göre $x < y$ olmak üzere I için bir gröbner bazı

$$G = \{x^2y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$$

$Q[x, y]_I$ için bir baz $1, x, y, x^2, xy$ 'nin kosetlerinden meydana gelir ve

$$\dim(Q[x, y]_I) = 5$$

$Q[x, y]/I$ için bir çarpım tablosu verelim.

$\times$	1	x	y	x^2	xy
1	1	x	y	x^2	xy
x	x	x^2	xy	$-y + 2x$	$y - x$
y	y	xy	$xy + x^2$	$y - x$	x
x^2	x^2	$-y + 2x$	$y - x$	$-xy + 2x^2$	$xy - x^2$
xy	xy	$y - x$	x	$xy - x^2$	x^2

Tablodaki bazı hesaplamalar aşağıdaki şekilde elde edilmiştir.

$$xy^2 \xrightarrow{G} x \quad N_G(xy^2) = x$$

$$(y + I)(xy + I) = x + I$$

$$\{1 + I, x + I, y + I, xy + I\}$$

Q bazıdır.

$$\text{Örneğin; } (2x^2 + y)(3xy - 5) = 6x^3y - 10x^2 + 3xy^2 - 5y$$

$$\equiv 6(xy - x^2) - 10x^2 + 3x - 5y = 6xy - 16x^2 - 5y + 3 \pmod{I}$$

$$(2x^2 + y + I)(3xy - 5 + I) = 6xy - 16x^2 - 5y + 3x + I$$

dir.

Örnek 3.3.5: $f_1 = x^2 + y^2 + 1$, $f_2 = x^2y + 2xy + x \in Z_5[x, y]$,

$$I = \langle f_1, f_2 \rangle \subseteq Z_5[x, y]$$

ve lex sıralamasına göre $x > y$ olsun. Örnek 3.3.2 den I için gröbner bazı

$\{g_1, g_2, g_3\}$ dir.

$$g_1 = f_1,$$

$$g_2 = xy + 3x + 2y^3 + 2y,$$

$$g_3 = y^5 + 2y^4 + 4y^2 + 4y + 2,$$

$Z_5[x, y] / I$ için bir baz $1, x, y, y^3, y^4$ ün kosetlerinden meydana gelir ve $\dim_{Z_5} \left(Z_5[x, y] / I \right) = 6$ dır.

Teorem 3.3.1. $V_{\bar{k}}(I) = \emptyset$ olması için gerek ve yeter koşul $1 \in G$ olmasıdır.

$f_1 = 0, f_2 = 0, \dots, f_5 = 0$ sisteminin $\bar{k}^n$ de çözümlerinin olmaması için gerek ve yeter koşul $G = \{1\}$ olmasıdır.

İspat: Weak Hilbert Nullstellensatz teoreminden $V_{\bar{k}}(I) = \emptyset$ olması için gerek ve yeter koşul $f \in I = k[x_1, x_2, \dots, x_n]$ idealinin tek indirgenmiş gröbner bazının $G = \{1\}$ olmasıdır.

Teorem 3.3.2: Aşağıdakiler birbirine denktir.

- (i) $V_{\bar{k}}(I)$, sonludur.
- (ii) Her $i = 1, 2, \dots, n$, $j \in \{1, 2, \dots, t\}$ ve bazı $v \in N$ için $lp(g_j) = x_j^v$ dır.
- (iii) $K[x_1, x_2, \dots, x_n] / I$ k-vektör uzayının boyutu sonludur.

İspat: $V_{\bar{k}}(I)$ sonlu olsun. $V_{\bar{k}}(I) = \emptyset$ olması için gerek ve yeter koşul $f \in I = k[x_1, x_2, \dots, x_n]$ ve $G = \{1\}$ olmasıdır.

$V_{\bar{k}}(I) \neq \emptyset$ ise $i \in \{1, 2, \dots, n\}, a_{ij}; j = 1, 2, \dots, \ell$ dir. $V_{\bar{k}}(I)$ deki noktaların i 'yinci koordinatları ve $\bar{k}$ tanımından $1 \leq j \leq \ell$ olacak şekilde her j için $0 \neq f_j \in k[x_i]$ ve $f_j(a_{ij}) = 0$ olsun.

$f = f_1 f_2 \dots f_\ell \in k[x_i] \subseteq k[x_1, x_2, \dots, x_n]$ ise Strong Hilbert Nullstellensatz Teoreminden $f \in I(V_{\bar{k}}(I))$ dir. $e \in N$, $f^e \in I$ olmak üzere bazı $lp(f^e) = x^{en}$ doğal sayıları için I 'nin her elemanının en büyük dereceli kuvvet çarpımı G 'nin bazı elemanlarının en büyük dereceli kuvvet çarpımı tarafından bölünür.

G 'de mevcut bir polinomun en büyük dereceli kuvvet çarpımı yalnız x_i 'nin bir kuvvetidir. Bu her $i = 1, 2, \dots, n$ için doğrudur.

$K[x_1, x_2, \dots, x_n] / I$ nin bir k – bazı, belirlenmiş G ile indirgenmiş kuvvet çarpımlarının kosetlerinin bir kümesidir.

Her $i = 1, 2, \dots, n$ için x_i 'nin bir kuvveti bazı g_i 'nin bir en büyük dereceli kuvvet çarpımıdır. Belirlenmiş G ile indirgenmiş sonlu birçok kuvvet çarpımı varsa ve böylece $\dim_{\bar{k}}(K[x_1, x_2, \dots, x_n] / I)$ sonludur.

$\dim_{\bar{k}}(K[x_1, x_2, \dots, x_n] / I)$ sonlu olsun. x_i 'nin $1, x_i, x_i^2, \dots$ kuvvetleri lineer bağımlıdır. Bundan dolayı bir m tamsayı olsun. $0 \leq j \leq m$ olacak şekilde $0 \neq c_j \in k$ için

$$\sum_{j=0}^m c_j x_i^j \in I$$

polinomu, $\bar{k}$ de sadece sonlu bazı köklere sahip olabilir. $V_{\bar{k}}(I)$ noktalarının i -yinci koordinatları için sadece sonlu bazı değerleri vardır. O halde $V_{\bar{k}}(I)$ sonludur.

Örnek 3.3.6: $Q[x, y]$ 'de $I = \langle x^2 y - y + x, xy^2 - x \rangle$ ideali için belirlenmiş $x < y$ olmak üzere deglex sıralamasına göre bir gröbner bazı Örnek 3.3.1 den

$$G = \{x^2 y - y + x, -y^2 + xy + x^2, x^3 + y - 2x\}$$

dir. x^3 ve y^4 , G 'nin elemanlarının bir en büyük dereceli kuvvet çarpımıdır ve böylece $V_{\bar{k}}(I)$ sonludur.

$$V_{\bar{Q}}(I) = \{(0, 0), (\alpha, -1), (-\alpha, 1), (\alpha', -1), (-\alpha', 1)\}$$

α ve α' , $z^2 - z - 1 = 0$ denkleminin kökleridir.

Örnek 3.3.7: $I = \langle f_1, f_2 \rangle \subseteq Z_5[x, y]$ için indirgenmiş gröbner bazı $\{g_1, g_2, g_3\}$ dir.

$$f_1 = x^2 + y^2 + 1, f_2 = x^2 y + 2xy + x$$

lex sıralamasına göre $x > y$ olsun. Örnek 3.3.2 den

$$g_1 = f_1$$

$$g_2 = xy + 3x + 2y^3 + 2y$$

$$g_3 = y^5 + 2y^4 + 4y^2 + 4y + 2$$

x^2 ve y^5 , en büyük dereceli kuvvet çarpımlarıdır ve $V_{Z_5}(I)$ sonludur.

Çözümlerin hepsi Z_5 'de olmayıp bazıları $\bar{Z}_5$ 'dedir.

Teorem 3.3.3: $I = \langle f_1, f_2, \dots, f_s \rangle \subset k[x_1, x_2, \dots, x_n]$ bir ideal ve w , bir bilinmeyen değer olsun.

$f \in \sqrt{I}$ olması için gerek ve yeter koşul $1 \in \langle f_1, f_2, \dots, f_s, 1 - wf \rangle \subseteq k[x_1, x_2, \dots, x_n, w]$ olmasıdır.

İspat: Hilbert Nullstellensatz Teoreminden

$I(V_{\bar{k}}(I)) = \sqrt{I}$ ve $f \in \sqrt{I}$ olması için gerek ve yeter koşul her $(a_1, a_2, \dots, a_n) \in V_{\bar{k}}(I)$ için $f(a_1, a_2, \dots, a_n) = 0$ olmasıdır.

Eğer $(a_1, a_2, \dots, a_n, b) \in V_{\bar{k}}(\langle f_1, f_2, \dots, f_s, 1 - wf \rangle)$ ise her $i = 1, 2, \dots, s$ için

$$f_i(a_1, a_2, \dots, a_n) = 0$$

ve

$$1 - b \cdot f(a_1, a_2, \dots, a_n) = 0 \text{ dir.}$$

Fakat $(a_1, a_2, \dots, a_n) \in V_{\bar{k}}(I)$ ve bundan dolayı

$$f(a_1, a_2, \dots, a_n) = 0$$

ve

$1 - b \cdot f(a_1, a_2, \dots, a_n) = 0$ dir. $1=0$ ifadesinden dolayı bir çelişki olur. Bu yüzden

$V_{\bar{k}}(\langle f_1, f_2, \dots, f_s, 1 - wf \rangle) = \emptyset$ dir ve Weak Hilbert Nullstellensatz Teoreminden

dolayı $1 \in \langle f_1, f_2, \dots, f_s, 1 - wf \rangle$ olur.

$$1 \in \langle f_1, f_2, \dots, f_s, 1 - wf \rangle \text{ olsun.}$$

Bazı $h_i, h \in k[x_1, x_2, \dots, x_n, w]$ için $1 = \sum_{i=1}^s h_i f_i + h(1 - wf)$ ve

Her $(a_1, a_2, \dots, a_n) \in V_{\bar{k}}(I)$ için $f_i(a_1, a_2, \dots, a_n) = 0$ dır.

$1 = (1 - wf(a_1, a_2, \dots, a_n))h(a_1, a_2, \dots, a_n, w)$ olur. $h(a_1, a_2, \dots, a_n, w)$, w 'ye bağlı bir polinomdur.

Eğer $f(a_1, a_2, \dots, a_n) \neq 0$ ise $w = \frac{1}{f(a_1, a_2, \dots, a_n)}$ olur ve böylece bir çelişki olur.

Bundan dolayı $f(a_1, a_2, \dots, a_n) = 0$ olur ve $f \in \sqrt{I}$ dir.

Örnek 3.3.8: $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle \subset Q[x, y]$ bir ideal olsun.

$f = y - x^2 + 1 \in \sqrt{I}$ olduğunu gösterelim.

$\langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - w(y - x^2 + 1) \rangle$, $Q[x, y, w]$ halkasında bir ideal olur.

$x < y < w$ olmak üzere deglex sıralamasına göre bu ideal için bir gröbner bazı $\{1\}$ dir.

$G = \{1\}$ olması için gerek ve yeter koşul $f \in \sqrt{I}$ olmasıdır. Böylece

$f \in \sqrt{I}$ olması için gerek ve yeter koşul bazı e 'ler için $f^e \in I$ olmasıdır.

Örneğin deglex sıralamasına göre $x < y$, $G = \{y^2, x^4 - 2x^2 + 1\}$ bir gröbner bazıdır.

Bu gröbner bazını $i = 1, 2, \dots$ için f^i 'nin normal formunu elde ederken kullanırız.

Normal formu sıfırdır.

$$N_G(f) = f \neq 0$$

$$N_G(f^2) = -2yx^2 + 2y \neq 0$$

fakat $N_G(f^3) = 0$ bu nedenle $f^3 \in I$ dır.

Teorem 3.3.4: I , $k[y_1, y_2, \dots, y_m, x_1, \dots, x_n]$ 'nin sıfırdan farklı bir ideali, " $<$ " bir eleme sıralaması, $x > y$ ve $G = \{g_1, g_2, \dots, g_t\}$ bu I ideali için bir gröbner bazı olsun.

$G \cap k[y_1, \dots, y_m]$, $I \cap k[y_1, \dots, y_m]$ ideali için bir gröbner bazıdır.

$I \cap k[y_1, \dots, y_m]$ idealine, x değişkenlerine elenmiş eleme ideali denir.

İspat: $G \cap k[y_1, \dots, y_m], I \cap k[y_1, \dots, y_m]$ tarafından içerilir.

$0 \neq f(y_1, \dots, y_m) \in I \cap k[y_1, \dots, y_m]$ olsun.

G, I için bir gröbner bazı olduğundan en az bir $g_i \in G$ için $lp(g_i)/lp(f)$ dir.

Ayrıca f , sadece y değişkenlerini içerir. g_i 'nin her terimi Lemma 3.3.1'den y değişkenlerini içerir.

$$g_i \in G \cap k[y_1, \dots, y_m]$$

Böylece her $f \in I \cap k[y_1, \dots, y_m]$ için $lp(g_i)/lp(f)$ olacak şekilde $g_i \in G \cap k[y_1, \dots, y_m]$ dir ve $G \cap k[y_1, \dots, y_m]$ ile $I \cap k[y_1, \dots, y_m]$ için bir gröbner bazıdır.

Önerme 3.3.3: I ve $J, k[x_1, x_2, \dots, x_n]$ de ideal ve w , bir değişken olsun. Eğer $\langle wI, (1-w)J \rangle, k[x_1, x_2, \dots, x_n]$ de ideal olursa

$$I \cap J = \langle wI, (1-w)J \rangle \cap k[x_1, \dots, x_n]$$

olur.

Önerme 3.3.4: Eğer $I = \langle f_1, f_2, \dots, f_s \rangle$ ve $J = \langle f'_1, f'_2, \dots, f'_s \rangle$ ise

$\langle wf_1, \dots, wf_s, (1-w)f'_1, \dots, (1-w)f'_s \rangle, \langle wI, (1-w)J \rangle$ ideali için bir üreteç kümesidir.

İspat: $f \in I \cap J$ olsun. O zaman

$$f = wf + (1-w)f \text{ olup}$$

$$f \in \langle wI, (1-w)J \rangle \cap k[x_1, \dots, x_n] \text{ dir. Böylece } f \in \langle wI, (1-w)J \rangle \subseteq k[x_1, \dots, x_n, w] \text{ dir.}$$

O halde

$$f(x_1, \dots, x_n) = \sum_{i=1}^s wf_i(x_1, \dots, x_n)h_i(x_1, \dots, x_n, w) + \sum_{j=1}^p (1-w)f'_j(x_1, \dots, x_n)h'_j(x_1, \dots, x_n, w)$$

$$w \notin f(x_1, x_2, \dots, x_n) \text{ dir.}$$

$$w=1 \text{ ise } f \in I$$

$$w=0 \text{ ise } f \in J \text{ dir.}$$

Örnek 3.3.9: $I = \langle x^2 + y^3 - 1, x - yx + 3 \rangle$ ve $J = \langle x^2 y - 1 \rangle$

$Q[x, y]$ 'de idealler olsun.

$$I = \langle w(x^2 + y^3 - 1), w(x - yx + 3), (1 - w)(x^2 y - 1) \rangle \subseteq Q[x, y, w]$$

ideali için bir G gröbner bazı elde edelim. $x > y$ olacak şekilde deglex sıralamasını x ile y üzerinde ve w, x ve y den büyük olacak şekilde eleme sıralamasını kullanalım.

$$G = \left\{ \begin{array}{l} x^3 y^2 - x^3 y - 3x^2 y - xy + x + 3, x^2 y^4 + x^4 y - x^2 y - y^3 - x^2 + 1, \\ 12853w + 118x^4 y + 9x^2 y^3 - 357x^3 y - 972x^2 y^2 + 2152x^2 y - 118x^2 - 9y^2 + 357x \\ + 972y - 2152, x^5 y + 3x^2 y^3 + 3x^2 y^2 - x^3 + 3x^2 y - 3y^2 - 3y - 3 \end{array} \right\}$$

$I \cap J$ ideali için bir gröbner bazı da

$$\left\{ \begin{array}{l} x^3 y^2 - x^3 y - 3x^2 y - xy + x + 3, x^2 y^4 + x^4 y - x^2 y - y^3 - x^2 + x^5 y + 3x^2 y^3 + 3x^2 y^2 \\ - x^3 + 3x^2 y - 3y^2 - 3y - 3 \end{array} \right\}$$

şeklindedir.

Lemma 3.3.1: $f, g \in k[x_1, x_2, \dots, x_n]$ için

$$\langle f \rangle \cap \langle g \rangle = \langle [f, g] \rangle \quad (3.2)$$

dır.

İspat: $\ell = [f, g]$, ℓ 'nin tanımından $\ell \in \langle f \rangle \cap \langle g \rangle$ olur.

$$h \in \langle f \rangle \cap \langle g \rangle \text{ bazı } a, b \in k[x_1, x_2, \dots, x_n] \text{ için } h = af = bg \text{ dir.}$$

Böylece f/h ve g/h , $[f, g]$ tanımından

$$\ell/h \text{ ise } h \in \langle \ell \rangle = \langle [f, g] \rangle, h = c.\ell \text{ dir. Buradan}$$

$(f_1, f_2, f_3) = (f_1, (f_2, f_3))$ olur. Böylece

$[f_1, f_2, f_3] = [f_1, [f_2, f_3]]$ olup

$\langle f_1 \rangle \cap \langle f_2 \rangle \cap \langle f_3 \rangle = \langle [f_1, f_2, f_3] \rangle$ elde edilir.

Örnek 3.3.10: $f = x^2y^2 - y^2 + x^2 - 1$, $g = xy^2 - y^2 - x + 1 \in Q[x, y]$ ve lex sıralamasına göre $w > x > y$ olsun.

$\langle wf, (1-w)g \rangle \subseteq Q[x, y, w]$ ideali için gröbner bazı

$$G = \left\{ \begin{array}{l} x^2y^4 - x^2 - y^4 + 1, -wxy^2 + wx + wy^2 - w + xy^2 - x - y^2 + 1, \\ 2wx^2 - 2w + x^2y^2 - x^2 - y^2 + 1 \end{array} \right\}$$

dir.

$$(f, g) = 1 - x^2 - y^4 + x^2y^4$$

Bölme algoritmasından $[f, g] = \frac{f \cdot g}{(f, g)} = x - 1$ dir.

I ve J , $k[x_1, x_2, \dots, x_n]$ de iki ideal olsun. $J : I = \{g \in k[x_1, x_2, \dots, x_n] \mid gI \subseteq J\}$

kümesi ideal olup bölüm ideali olarak adlandırılır.

Lemma 3.3.2: $I = \langle f_1, f_2, \dots, f_s \rangle$ ve $J = \langle f'_1, f'_2, \dots, f'_s \rangle$, $k[x_1, x_2, \dots, x_n]$ de idealler olsun.

$$J : I = \bigcap_{i=1}^s J : \langle f_i \rangle \quad (3.3)$$

dir.

İspat: Eğer $g \in J : I$ ise $gI \subseteq J$, $i = 1, 2, \dots, s$ için $gf_i \in J$ ve böylece

$$g \in \bigcap_{i=1}^s J : \langle f_i \rangle$$

dir.

$g \in \bigcap_{i=1}^s J : \langle f_i \rangle$ olsun. O zaman $i = 1, 2, \dots, s$ için $g \langle f_i \rangle \subseteq J$ olup $gI \subseteq J$ olur.

Böylece $g \in J : I$ dir.

Lemma 3.3.3: J , bir ideal ve $f \neq 0$, $k[x_1, x_2, \dots, x_n]$ 'de bir polinom olsun. O zaman

$$J : \langle f \rangle = \frac{1}{f} (J \cap \langle f \rangle) \quad (3.4)$$

dir.

İspat: $g \in \frac{1}{f} (J \cap \langle f \rangle)$, $gf \in J$ dir. Böylece $g \in J : \langle f \rangle$ olur.

$$(g, f \in \langle f \rangle, g \langle f \rangle \subseteq J)$$

$g \in J : \langle f \rangle$ ise $gf \in J$, $g \langle f \rangle \subseteq J$ dir. Böylece $gf \in J \cap \langle f \rangle$ olur.

$$J : \langle f \rangle = \frac{1}{f} (J \cap \langle f \rangle)$$

dir.

Örnek 3.3.11: $g_1 = x(x+y)^2$, $g_2 = y$, $f_1 = x^2$, $f_2 = x+y \in Q[x, y]$

$I = \langle f_1, f_2 \rangle$ ve $J = \langle g_1, g_2 \rangle$ olsun.

$J : I$ ni bulalım.

Lemma 3.3.2.den

$$J : I = (J : \langle f_1 \rangle) \cap (J : \langle f_2 \rangle) \text{ ve}$$

$$J : I = \frac{1}{f_1} (J \cap \langle f_1 \rangle) \cap \frac{1}{f_2} (J \cap \langle f_2 \rangle) \text{ dir.}$$

$$\langle wg_1, wg_2, (1-w)f_1 \rangle \subseteq Q[x, y, w]$$

ideali için lex sıralaması $w > x > y$ göre $G_1 = \{x^2w - x^2, wy, x^3, x^2y\}$ gröbner bazıdır.

$$\frac{1}{f_1}(J \cap \langle f_1 \rangle) = \langle x, y \rangle$$

$\langle wg_1, wg_2, (1-w)f_2 \rangle \subseteq Q[x, y, w]$ ideali için $G_2 = \{wx - x - y, wy, x^3 + y^3, xy + y^2\}$ gröbner bazıdır ve

$$\frac{1}{f_2}(J \cap \langle f_2 \rangle) = \langle x^2 - xy + y^2, y \rangle$$

dir.

Sonuç olarak

$$\langle wx, wy, (1-w)(x^2 - xy + y^2), (1-w)y \rangle \subseteq Q[x, y, w] \text{ ideali için gröbner bazı}$$

$$G = \{wx, x^2, y\} \text{ dir.}$$

Böylece

$$J : I = \langle x^2, y \rangle \text{ olur.}$$

4. PİK İNDİRGEME TEKNİĞİ

4.1. Değişmeli Cebirde Pik İndirgeme Tekniği

Bu bölümde değişmeli cebir ve afin cebir geometride pik indirgeme tekniğinin ilk uygulamalarını göreceğiz.

Bu teknik genellikle verilen bir T dönüşümler grubunun işlemi altında verilen bir P nesnesinin kompleksinin kanonik formunun bazı türlerini bulmada kullanılır.

Bu düşünce oldukça basittir. Öncelikle P nesnesinin kompleksi seçilir. P nin kononik formu olan P' nesnesi bütün $t(p)$ ($t \in T$) nesneleri arasında kompleksi minimal olandır.

P nesnesinin bir P' kanonik modelini bulurken ilk önce uygun basit dönüşümlerin bir dizisi oluşturulur. Böylece bir nesnenin kompleksi her adımda azalır. Böyle bir dizi oluşturmak mümkündür. Bunun için pik indirgemesi kullanılır.

Değişmeli cebirde nesneler polinomlar, onların kompleksi ise onların dereceleridir. Dönüşümlerin grubu polinom otomorfizmlerinin bir grubu olup basit dönüşümler ise temel ve lineer otomorfizmlerdir.

$K[x, y]$, K cismi üzerinde iki değişkenli polinom cebiri olsun.

Teorem 4.1.1: $p(x, y) = ax^n + by^m + \sum_{im+jn \leq mn} c_{ij} x^i y^j$, $a, b, c_{ij} \in K$, $i, j > 0$, $a, b \neq 0$

ve $q(x, y) = Ax^r + By^s + \sum_{is+jr \leq rs} b_{ij} x^i y^j$, $A, B, b_{ij} \in K$, $i, j > 0$, $A, B \neq 0$ olsun.

Varsayalım m, n 'yi n , m 'yi s , r 'yi r , s 'yi bölmesin. $\max(m, n) \neq \max(r, s)$ olsun. O halde $p(x, y)$ 'yi $q(x, y)$ 'ye dönüştüren bir $\alpha \in \text{Aut}(K[x, y])$ otomorfizmi yoktur. Bazı özel durumlarda m/n veya n/m olan polinomlar alınabilir. Örneğin verilen bir polinomun fiberi bir $x = u(t)$, $y = v(t)$ bir değişkenli polinom parametresi olarak kabul edilirse bu durum mümkündür.

Önerme 4.1.1: $p, q \in C[x, y]$ gibi iki polinomun $\{p(x, y) = 0\}$, $\{q(x, y) = 0\}$ fiberlerinin bir değişkenli polinom parametresine sahip olduğunu kabul edelim.

O zaman eğer $C[x, y]$ 'nin p 'yi q 'ya dönüştüren bir $\alpha \in \text{Aut}(C[x, y])$ otomorfizmi varsa bu otomorfizm bulunabilir.

Özellikle eğer verilen polinomun fiberi bir basit birleşen eğri ise Lin ve Zaidenberg'in [16] iyi bilinen teoremi gereğince bu fiber bir değişkenli polinom parametresi kabul edilir.

$K = C$ durumunda her polinomu $x^k - y^\ell$, $(k, \ell) = 1$ formunda bir kanonik modeli vardır.

Teorem 4.1.2: $p(x, y) \in C[x, y]$, fiberi $\{p(x, y) = 0\}$ olan bir polinom olsun. O zaman $C[x, y]$ 'nin bazı otomorfizmleri $p(x, y)$ 'i $x^k - y^\ell$ ye $(k, \ell) = 1$ dönüştürür.

- a) $\max(k, \ell) \leq \deg(p(x, y))$
- b) $k/\deg(p(x, y))$ veya $\ell/\deg(p(x, y))$
- c) $p(x, y)$ 'nin Newton poligonu bir üçgen veya bir doğru parçasıdır.

$p(x, y)$, $ax^n + by^m + \sum_{im+jn \leq mn} c_{ij}x^i y^j$, $i, j > 0, a, b \neq 0$. Eğer $m, n \neq 0$ ise $m = k$ veya $m = \ell$ ve $n = \ell$ veya $n = k$ dir.

Aksi takdirde $p(x, y)$ lineer veya $ax^n + by^m + \sum_{im+jn \leq mn} c_{ij}x^i y^j$ en büyük dereceli kısmı bazı diğer polinomun uygun kuvvetidir.

Teorem 4.1.3: $p \in C[x, y]$, sabit bir polinom ve $\emptyset \in \text{Aut}(C[X, Y])$ olsun. O zaman $\emptyset$ 'nin $\emptyset_1, \emptyset_2, \dots, \emptyset_n$ elemanter ve lineer otomorfizmler olmak üzere öyle bir $\emptyset_1 \emptyset_2 \dots \emptyset_n$ parçalanışı vardır ki $p_i = \emptyset_1 \emptyset_2 \dots \emptyset_n(p)$, $i = 1, 2, \dots, n$ ve $p_0 = p$ olup

$$\deg(p_0) \geq \deg(p_k) \leq \dots \leq \deg(p_n), \quad 0 \leq k \leq n \text{ dir.}$$

Ayrıca $\deg(p_{i-1}) = \deg(p_i)$ olacak şekilde en çok bir $\emptyset_i$ vardır ve $\deg(p_i), \deg(p_k)$ 'nin minimal derecesidir.

Bu sonuç verilen bir polinomun kanonik modelini bulmak için bir yöntemdir. Bu yöntemle bir p polinomu verildiğinde eğer varsa $\deg(p)$ 'yi azaltan bir temel otomorfizm varlığını kontrol ederiz. Yani bu yöntem

$$\{x \longrightarrow x, y \longrightarrow \lambda_1 y + \lambda_2 x^k\}$$

ve

$$\{x \longrightarrow \lambda_1 x + \lambda_2 y^k, y \longrightarrow y\}$$

formundaki otomorfizmlerin varlığını kontrol etmemizi sağlar. Bu şekilde bir elemanter otomorfizmi kontrol etmek için λ_1, λ_2 ye bağlı bir polinom denkleminin bir çözüme sahip olduğunu göstermek gerekir. Bu ise gröbner bazı kullanılarak yapılabilir.

Eğer dereceyi azaltan bir temel otomorfizm yoksa Teorem 4.1.1'den bir kanonik model vardır.

$K[x, y]$ 'nin her otomorfizmi temel ve lineer otomorfizmlerin bir çarpımı olduğu Jung ve Van Der Kulk'un iyi bilinen bir sonucudur.

Her adımda dereceyi azaltacak temel ve lineer otomorfizmlerin bir dizisi bulunarak verilen bir polinomun kanonik modelini elde etmek istiyoruz. En son bulunan polinom derecesi azaltılamıyorsa bir kanonik model olacaktır. Bunu yapmak için iki durum söz konusudur. Birincisi $K[t] \times K[t]$ temel dönüşümleriyle $K[x, y]$ 'nin temel otomorfizmleri belirlenir. İkincisi $K[t] \times K[t]$ 'nin temel dönüşümlerinin bir sırasını düzenlemek için Whitehead [14]'nin pik indirgeme tekniği kullanılır. Böylece maksimum derece her adımda azaltılır.

4.2. Temel Otomorfizm ve PİK İndirgemesi

Önerme 4.2.1: $K[x, y]$ 'nin her otomorfizmi

$$x \longrightarrow x + f(y); y \longrightarrow y$$

formundaki otomorfizmlerin ve lineer otomorfizmlerin bir çarpımıdır. (g_1, g_2) , $\deg(g_1) \geq \deg(g_2)$ olacak şekilde $K[x, y]$ 'nin bir otomorfizmi ise (g_1, g_2) bir lineer otomorfizm veya bir $\mu \in K^*$ ve bir d pozitif tamsayısı için $\deg(g_1 - \mu g_2^d) < \deg(g_1)$ dir.

Önerme 4.2.2: $(u, v) \in K[t] \times K[t]$ aşağıdaki elemanter dönüşümlerin bir dizisi (u, v) 'yi $(\hat{u}, \hat{v})$ 'ye dönüştürür.

(i) Bu diziyeye göre polinomların maksimum dereceleri her adımda azalır.

(ii) ET lerin dizisiyle (u', v') de maksimum dereceler azalmaz

(i) Eğer u ve v aynı en büyük dereceli terimlere sahip ise $(u, v) \longrightarrow (u - v, v)$ dönüşümü ile maksimum dereceler azalır.

İspat: ET 'nin bir dizisi azalmadan önce maksimum dereceyi yükseltiyor veya olduğu gibi bırakıyorsa bu dizide ET 'nin bir çift alt dizisi olmalıdır. Bu çiftin biri maksimum dereceyi artırır veya olduğu gibi bırakır ve diğeri ise onu azaltır. Sonuç olarak pik her zaman azaltılabilir. Başka bir deyişle maksimum derece ET 'nin bir dizisi ile azaltılabilir. Maksimum derece tek bir ET ile de azaltılabilir.

$$(u, v) \in K[t] \times K[t] \text{ polinomların bir çifti ve } \deg(u) \leq \deg(v), \alpha_1 \text{ ve } \alpha_2$$

ET 'nin iki alt dizisi olsun.

$$ET (1) \alpha_1 : (u, v) \longrightarrow (u + \mu.v^k, v); \mu \in K^*, k \geq 2$$

α_1 , $\deg(u) \leq \deg(v)$ olduğundan maksimum dereceyi artırır. Bu durumda bir

lineer ET maksimum dereceyi azaltamadığından α_2 için iki durum söz konusudur.

(a) $\alpha_2 : (u + \mu.v^k, v) \longrightarrow (u + \mu.v^k, v + \lambda(u + \mu.v^k)^m); \lambda \in K^*, k \geq 2$ maksimum derece artar. Bu da varsayımımızla çelişir.

(b) $\alpha_2 : (u + \mu.v^k, v) \longrightarrow (u + \mu.v^k + \lambda.v^m, v)$, α_2 'nin maksimum dereceyi azaltması için $\mu.v^k = -\lambda.v^m$ olmalıdır. Bu durumda $\alpha_2 = \alpha_1^{-1}$ olup pik indirgemesi α_1 ve α_2 'nin etkisini kısaltır. ($\alpha_1.\alpha_2 = \alpha_1.\alpha_1^{-1} = 1$)

$$ET(2) \quad \alpha_1 : (u, v) \longrightarrow (u, v + \mu.u^k); \mu \in K^*, k \geq 2$$

Eğer $\deg(v + \mu.u^k) = \deg(u^k)$ ise α_1 , maksimum dereceyi artırır. $\deg(u) \leq \deg(v)$ olduğundan α_1 , maksimum dereceyi değiştirmeyecek şekilde α_2 için iki durum söz konusudur.

$$(a) \quad \alpha_2 : (u, v + \mu.u^k) \longrightarrow (u, v + \mu.u^k + \lambda.u^m)$$

Eğer α_2 maksimum dereceyi azaltırsa $m \geq k$ olacaktır. Eğer $m = k$ ise $\alpha_1.\alpha_2$, bir tek ET ye eşittir. $\deg(u^k) = k.\deg(u)$, $\deg(u^m) = m.\deg(u)$ $m = k$ 'nin uygun seçimiyle $\deg(v + \mu.u^k + \lambda.u^m) < \deg(v + \mu.u^k)$

Eğer $m > k$ ise α_2 'nin maksimum dereceyi azaltması için $\deg(u)/\deg(v)$ olmalıdır. Bu durumda α_2 tek başına (u, v) 'nin maksimum derecesini azaltır.

(b) $\alpha_2 : (u, v + \mu.u^k) \longrightarrow (u + \lambda.(v + \mu.u^k)^m, v + \mu.u^k)$; α_2 , bu çiftte ilk polinomun derecesini değiştirir ve bu maksimum derece değildir.

$ET(3) \quad \alpha_1$, lineer olmak üzere

$\alpha_1 : (u, v) \longrightarrow (a_1.u + a_2.v, b_1.u + b_2.v)$; $a_1, a_2, b_1, b_2 \in K$ için iki durum söz konusudur.

$$(a) \quad \alpha_2 : (a_1.u + a_2.v, b_1.u + b_2.v) \longrightarrow (a_1.u + a_2.v, b_1.u + b_2.v + \mu.(a_1.u + a_2.v)^k)$$

$k = 1$ ise α_2 lineer ve $\alpha_1.\alpha_2$, yalnız bir ET dir.

$k > 1$ ise α_2 maksimum derecesini azaltacak şekilde $a_2 = 0$ olmalıdır. Bu durumda bir tek ET ile (u, v) 'nin maksimum derecesi azalır.

(b) ($ET(1)$)'in α_2 içinde durum benzerdir. α_2 'nin ($ET(1)$) tipinde olması durumu tamamen aynıdır.

Böylece yukarıdaki durumların her biri düşünüldüğünde eğer pik indirgemesi varsa dizideki ET lerin sayısını azaltabiliriz.

Önerme 4.2.3: $p(x, y) = ax^n + by^m + \sum_{im+jn \leq mn} c_{ij} x^i y^j$; $a, b, c_{ij} \in K$, $i, j > 0, a, b \neq 0$

olsun. m , n 'yi n , m 'yi bölsün. O zaman $p(x, y)$ 'nin derecesini azaltabilecek $\alpha \in \text{Aut}(K[x, y])$ otomorfizmi yoktur.

Önerme 4.2.4: $p(x, y) = ax^n + by^m + \sum_{im+jn \leq mn} c_{ij} x^i y^j$; $a, b, c_{ij} \in K$, $i, j > 0, a, b \neq 0$

formunda bir polinom olsun.

Bir β elemanter veya lineer otomorfizm, $p(x, y)$ 'e uygulanarak aynı formda bir polinom elde edilir. m/n veya n/m durumlarda $m = kn$ olur ve

$$\beta : x \longrightarrow x + \mu \cdot y^k ; y \longrightarrow y, \mu \in K^*$$

dir.

İspat: Bu durum bir lineer otomorfizm için açıktır. β , bir elemanter otomorfizm olsun. O zaman

$$\beta : x \longrightarrow x + \mu \cdot y^k ; y \longrightarrow y, \mu \in K^*, k \geq 2 \quad (4.1)$$

$$\begin{aligned} \beta(p(x, y)) &= ax^n + a\mu^n y^{kn} + by^m + \sum_{i=1}^{n-1} b_{ij} x^i y^{k(n-i)} + \sum_{im+jn \leq mn} c_{ij} (x^i + \mu^i y^{ki+j}) \\ &+ \sum_{s=1}^{i-1} a_{ij} x^s y^{k(i-s)+j} \end{aligned}$$

Burada üç durum söz konusudur.

$kn < m$ (4.1) de $x^i y^j$ 'nin her monomialinin $im + jn \leq mn$ ye sahip olduğunu göstermeliyiz.

$x^s y^{k(i-s)+j}$ formundaki monomialler için bu durum açık değildir.

$$km + (k(i-s) + j)n = sm + kn(i-s) + jn$$

$kn < m$ olduğundan $km + kn(i-s) < sm + m(i-s)$ olur. Bu yüzden

$$km + (k(i-s) + j)n < mi + nj \leq mn$$

$kn > m$ bu durumda $\beta(p(x, y))$ 'nin en büyük dereceli kısmı $ax^n + a\mu^n y^{kn}$, (4.1) deki her $x^i y^j$ monomialinin $ikn + jn \leq kn^2$ sahip olduğunu göstermeliyiz. $x^s y^{k(i-s)+j}$ formundaki monomialler için

$$skn + (k(i-s) + j)n = kni + jn \quad (4.2)$$

olduğunu göstermeliyiz. $im + jn \leq mn$ nin her iki tarafını $\frac{kn}{m}$ ile çarpalım.

$$\frac{kn}{m}(mi + nj) \leq \frac{kn}{m}.mn$$

$$kni + \frac{kn^2 j}{m} \leq kn^2$$

$$kn > m \text{ olduğundan } \frac{kn^2}{m} > n$$

$$kni + jn \leq kn^2$$

Bu durumda (4.2)'ün ispatı tamamlanmış olur.

(c) $kn = m$ en büyük dereceli terim olan y^m 'i yok eden $\beta: x \longrightarrow x + \mu.y^k; y \longrightarrow y, \mu \in K^*$ olması durumu dışındaki ET ler için önceki durumlar söz konusu olur.

Önerme 4.2.3 ispatı : $p(x, y)$ 'i $q(x, y)$ 'e dönüştüren bir $\alpha \in \text{Aut}(K[x, y])$ kabul edelim. $p(x, y)$ polinomunu bir değişkenli parametrik polinom şeklinde yazalım. O zaman $(p(0, t), p(t, 0)) \in K[t] \times K[t]$ olur.

Temel otomorfizmlerin bir dizisinde α otomorfizmine uygun gelecek polinomun derecesini azaltacak bir elemanter otomorfizm olmalıdır. Elemanter otomorfizmler dizisinde dereceyi azaltan elemanter otomorfizmin uygulanabileceği ilk yer bulunmalıdır. Bu otomorfizmin

$$\beta: x \longrightarrow x + \mu.y^k; y \longrightarrow y, \mu \in K^*$$

formunda ve bir $\tilde{p}(x, y)$ polinomuna uygulandığını varsayalım.

$$\tilde{p}(x, y) = \tilde{a}x^{\tilde{n}} + \tilde{b}y^{\tilde{m}} + \sum_{i\tilde{m}+j\tilde{n}\leq\tilde{m}\tilde{n}} \tilde{c}_{ij}x^i y^j \text{ olsun.}$$

$\tilde{p}(x, y)$ polinomunun derecesini azaltan β otomorfizm uygulanarak $\tilde{k}.\tilde{n} = \tilde{m}$ ve $v \in K^*$ dur. $(v, \tilde{b}\tilde{a}^{-k})$ olabilir

$(u, v) \longrightarrow (u + v.v^k, v)$ formundaki ET 'nin $(\tilde{p}(0, t), \tilde{p}(t, 0))$ polinomlarının çiftine uygulanarak derecelerinin maksimumu azalır.

Önerme 4.2.2 den $(p(0, t), p(t, 0))$ polinomların maksimum derecelerini azaltan bir ET vardır. Bununla birlikte verilen Önerme 4.1.1'in hipotezi bunun mümkün olmadığını gösterir.

Önerme 4.1.1 ispatı: Öncelikle p ve q 'nun her ikisinin $C[x, y]$ 'nin otomorfizmleriyle dereceleri azaltılamayan kanonik modellere sahip olduğunu göstermeliyiz. Polinomların her ikisi

$$ax^n + by^m + \sum_{i\tilde{m}+j\tilde{n}\leq\tilde{m}\tilde{n}} c_{ij}x^i y^j ; m, n \geq 0 \quad (4.3)$$

formundadır. Eğer m/n veya n/m ise uygulanan bir elemanter otomorfizm ile polinomun derecesini azaltabiliriz. Bu elemanter otomorfizm kolayca bulunabilir. Eğer $kn = m$ ise $\beta: x \longrightarrow x + \mu.y^k; y \longrightarrow y, \mu = \sqrt[n]{-b}$ otomorfizmi uygulanır. Bu şekilde devam ederek $(m < n)$ (4) formunda bir polinom elde edilir. Diğer polinomda dereceleri m' ve n' aynı forma azaltılır.

$m' < n'$ kabul edelim. Eğer $n' = n$, (Teorem 4.1.1 ile) $p(x, y)$ 'i $q(x, y)$ 'ye dönüştüren $C[x, y]$ 'nin otomorfizmi yoktur. Eğer $n' = n$ ise p 'ye q 'ya dönüştüren bir otomorfizm olması için gerek ve yeter koşul $\{x \longrightarrow x, y \longrightarrow y + f(x)\}, \deg(f) < \frac{m}{n}$ formundaki bazı otomorfizmler ile bir lineer otomorfizmin bileşkesi p 'yi q 'ya dönüştürebilir olmasıdır.

Eğer bu mümkünse $f(x)$ polinomunun sabitlerini düşünmeliyiz. Polinom denklemlerinin bir sisteminin C 'de bir çözümü vardır. Gröbner bazının iyi bilinen algoritması uygulanarak yapılabilir. Bu algoritma genellikle yavaştır. Bununla birlikte Önerme 4.1.1 özel durumu vardır. Tamamında bu algoritmayı uygulamak zorunda değiliz. Bu durumda eğer verilen polinom bir koordinat yani x 'in otomorfik görüntüsü ise mümkündür. Bu durumda (4.3) formunda bir polinom alındığında polinomun düzenli olması için gerek ve yeter koşul $\max(m, n) = 1$ olmasıdır.

Teorem 4.1.2 ispatı: Zaidenberg ve Lin [16] nin bir sonucuna göre $C[x, y]$ 'nin bazı otomorfizmleri $p(x, y)$ 'i $x^k - y^\ell$ 'e $(k, \ell) = 1$ götürür. $\{x^k - y^\ell = 0\}$ polinom fiberinin bir değişkenli parametrizasyonu $x = t^\ell, y = t^k$ dir. Bu yüzden baştaki açıklama ile $\{p(x, y) = 0\}$ fiberi $x = u(t), y = v(t)$ parametrelili kabul edilir ve bir ET dizisi $(u(t), v(t))$ 'i (t^ℓ, t^k) 'ya dönüştürür. Böylece maksimum dereceler bir polinomlar çiftinde her adımda azalır bazen maksimum derece birkaç adımda değişmez. (Teorem 4.1.2 nin (a) ve (c) ispatı tamamlandı.) ET dizisinde geçen ET maksimum dereceyi azaltır. O zaman dizideki maksimum dereceyi azaltan son ET alınır. Yani bu ET nin uygulamasından sonra derecelenir. Böylece $\{k, k\}, \{k, \ell\}, \{\ell, \ell\}$ olan bir polinom çifti elde edilir.

Yani bir polinom çiftinin en az birinin $\{km, k\}$ veya $\{\ell, m\ell\}$ ($m \geq 2$) dir. Bu durumda k veya ℓ polinomlar çiftinde maksimum dereceyi böldüklerinden iki değişkenli polinomun derecesini de bölerler.

Teoremin (b) kısmı benzer şekilde ispatlanır.

4.3. Polinom Otomorfizmlerinin Grubunun Parçalanışı

Bu bölümde, arttırma ile bir serbest çarpımda $Aut(K[x, y])$ grubunun yeni bir parçalanışını üretmek için pik indirgeme metodunun bir uygulamasını vereceğiz.

Arttırma ile serbest çarpımda bunu izleyen iyi bilinen analizler vardır.

$$Aut(K[x, y]) = Af *_{Af \cap \ddot{U}\ddot{U}} \ddot{U}\ddot{U} = Af *_{Af \cap A\ddot{U}} A\ddot{U} \quad (4.4)$$

Analizimiz daha simetrik bir forma sahiptir.

Teorem 4. 3.1.

$$Aut(K[x, y]) = T\ddot{U}\ddot{U} *_{T\ddot{U}\ddot{U} \cap TA\ddot{U}} TA\ddot{U} = T\ddot{U}\ddot{U} *_{Af} TA\ddot{U} \quad (4.5)$$

Yöntemimizin diğer modeli olarak $T\ddot{U}\ddot{U}$ ve $TA\ddot{U}$ gruplarının içindeki lineer olmayan otomorfizmlerini ayıracağız.

$K[x, y]$ 'de polinomların çiftine uygulanan ET leri tanımlayalım.

$$(E1) (u, v) \longrightarrow (u + a.v^k, v); a \in K^*, k \geq 2$$

$$(E2) (u, v) \longrightarrow (u, v + a.u^k)$$

(E3) Afin dönüşümler

$$(u, v) \longrightarrow (a_1u + a_2v + c_1, b_1u + b_2v + c_2); a_1, a_2, b_1, b_2, c_1, c_2 \in K$$

Bu elemanter dönüşümler Jung ve Vander Kulk un teoremi ile $Aut(K[x, y])$ 'e izomorfik olan bir grup üretir.

Lemma 4.3.1. (E1) ve (E2)'nin dönüşümleri tarafından üretilen grup (E1) dönüşümleri tarafından üretilen alt grubu ile (E2) dönüşümleri tarafından üretilen alt grubunun bir serbest çarpımıdır. Bu altgruplar abelyendir.

İspat: İspatı yaparken pik indirgeme tekniğini kullanacağız. Yani

ET 'nin bir dizisi azalmadan önce (ET 1 veya ET 2) maksimum dereceyi yükseltiyor veya olduğu gibi bırakıyorsa dizide ET 'nin bir çift alt dizisi olmalıdır. Bu çiftin biri maksimum dereceyi artırır veya olduğu gibi bırakır ve diğeri ise onu azaltır. Sonuç olarak pik her zaman azaltılabilir. (u, v) , $K[x, y]$ 'nin polinomlarının bir çifti ve $\deg u \leq \deg v$ ve α_1 ve α_2 , (u, v) 'ye uygulanan ET nin iki alt dizisi olsun.

$$(1) \alpha_1 : (u, v) \longrightarrow (u + a.v^k, v); a \in K^*, k \geq 2$$

α_1 , kabulümüz $\deg u \leq \deg v$ olduğundan maksimum dereceyi artırır. Bu durumda α_2 için iki durum söz konusudur.

(a) $\alpha_2 : (u + \mu.v^k, v) \longrightarrow (u + \mu.v^k, v + b.(u + \mu.v^k)^m); b \in K^*, m \geq 2$ maksimum derece artar bu da kabulümüzle çelişir.

$$(b) \alpha_2 : (u + \mu.v^k, v) \longrightarrow (u + \mu.v^k + b.v^m, v)$$

α_2 'nin maksimum dereceyi azaltması için $\mu.v^k = -b.v^m$ olmalıdır. Bu durumda $\alpha_2 = \alpha_1^{-1}$ olup pik indirgemesi α_1 ve α_2 'nin etkisini kısaltır.

$$(2) \alpha_1 : (u, v) \longrightarrow (u, v + a.u^k); a \in K^*, k \geq 2$$

Eğer $\deg(v + a.u^k) = \deg(u^k)$ ise α_1 maksimum dereceyi artırır. Bununla birlikte $\deg u \leq \deg v$ olduğundan α_1 , maksimum dereceyi değiştirmeyecek şekildedir. O halde α_2 için iki durum söz konusudur.

$$(a) \alpha_2 : (u, v + a.u^k) \longrightarrow (u, v + a.u^k + b.u^m)$$

Eğer α_2 maksimum dereceyi azaltırsa $m \geq k$ olacaktır. Eğer $m = k$ ise $\alpha_1 \alpha_2$, bir tek ET ye eşittir. Eğer $m > k$ ise, α_2 maksimum dereceyi azaltması için $\deg u / \deg v$ olmalıdır. Bu durumda α_2 tek başına (u, v) 'nin maksimum derecesini azaltır. α_1 ve α_2 değiştirilebilir.

$$(b) \alpha_2 : (u, v + a.u^k) \longrightarrow (u + b.(v + a.u^k)^m, v + a.u^k)$$

α_2 , bu çiftte ilk polinomun derecesini değiştirir ve bu maksimum derece değildir. Böylece ET nin bir çarpımı verildiğinde $\alpha^{-1} \alpha$ formundaki ET 1 veya ET 2 nin ET çiftlerinin etkisini kısaltır. Aynı tipin ET leri değiştirilip ET nin diğer

çarpımını verir. Aynı otomorfizm, T ile verilmiş polinomların bir çiftinin maksimum derecesini azaltır. Polinomlar $(T(x), T(y))$ ile başlanıp, (x, y) çifti ile biter. Her adımda, seçilen ET , maksimum derecesini azaltabilir ve tektir.

KAYNAKLAR

- [1] ABHYANKAR, S.S. VE MOH, T.-T., (1975). Embeddings of the line in the plane, J. Reine Angew. Math. 276 , 148-166.
- [2] ADAMS, W. VE LOUSTAUNAU, P., (1994). An introduction to Gröbner bases. American Mathematical Society, Providence.
- [3] COHN, P.M.,(1985). Free Rings and Their Relations. 2nd Ed. Academic Press, London.
- [4] DICKS, W., Automorphisms of the polynomial ring in two variables, (1983). Publ. Sec. Mat. Univ. Autònoma Barcelona 27 ,155-162.
- [5] DRENSKY, V. VE YU, J.-T., Tame and wild coordinates of $K[[x, y]]$ Trans. Amer. Math. Soc., to appear.
- [6] EISENBUD, D. VE NEUMANN, W.D. Three-dimensional link theory and invariants of plane curve singularities. Ann. Math. Stud.110, Princeton. Princeton Univ. Press.
- [7] NAGAO, H., On $GL(2, K[x])$, (1959) J. Inst. Polytech. Osaka City Univ. Ser. A 10, 117-121.
- [8] NEUMANN, W.D. VE WIGHTWICK, P.G. Algorithms for polynomials in two variables, this volume.
- [9] SHAFAREVICH, I.R., (1966). On some infinite dimensional groups, Rend. Mat. e Appl. 25, 208-212.
- [10] SHPILRAIN, V. VE YU, J.-T. (1997). Polynomial automorphisms and Gröbner reductions, J. Algebra 197 , 546-558.
- [11] SHPILRAIN, V. VE YU, J.-T., (1998). On generators of polynomial algebras in two commuting or non-commuting variables, J. Pure Appl. Algebra 132 , 309-315.
- [12] SHPILRAIN, V. VE YU, J.-T., (1999). Embeddings of curves in the plane, J. Algebra 217, 668-678.

- [13] SHPILRAIN, V. VE YU, J.-T., (1999). Peak reduction technique in commutative algebra.
- [14] WHITEHEAD, J.H.C., (1936). On equivalent sets of elements in a free group, Ann. Of Math. 37, 782-800.
- [15] WRIGHT, D., (1978). The amalgamated free product structure of $GL(k[X_1, X_2, \dots, X_n])$ and the weak Jacobian theorem for two variables, J. Pure Appl. Algebra 12, 235-251.
- [16] ZÄIDENBERG, M.G. VE LIN, V.YA., (1983). An irreducible, simply connected algebraic curve in C^2 is equivalent to a quasihomogeneous curve, Soviet Math. Dokl. 28, 200-204.

ÖZGEÇMİŞ

1980 yılında Antakya’da doğdum. Öğrenimimi sırasıyla Aşağıokçular Köyü İlkokulu, Fatih Sultan Mehmet Ortaokulu ve Antakya Kurtuluş Lisesi’nde tamamladım. 1997 yılında Ankara Üniversitesi Fen Fakültesi Matematik Bölümü’ne girdim. 2001 yılında lisans öğrenimimi tamamlayıp 2002 yılında Matematik Öğretmeni olarak görev yapmaya başladım. 2006 yılında Çukurova Üniversitesi Matematik bölümünde yüksek lisansa başladım. 2007 yılında MEB Yurtdışı Bursunu kazanıp master ve doktora yapmak için İngiltere’ye gönderirdim ve halen İngiltere’deki eğitimime devam etmekteyim.